TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ SOLO INFORMAZIONE E ARTICOLI **2€**

n. 171

HACKER JOURNAL

www.hackerjournal.it



HACKING
COLD BOOT: ATTACCO A FREDDO

ATTUALITÀ
NELLE FAUCI DI EBAY

PROGRAMMING
IL COMPUTER CI GUARDA

ANONIMITY
MAIL ANONIMA? SI PUÒ (ANCORA) FARE

MOBILE
SMARTPHONE CAMBIA CANALE

TUNELLING
AGGIRIAMO FILTRI E FIREWALL

QUATTORD. ANNO 9 - N° 171 - 5/18 MARZO 2009 - € 2,00

WLF PUBLISHING

Anno 9 – N.171
5/18 marzo 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Il mondo a due velocità

"Un animo forte è quello che anche nelle più forti emozioni non perde il proprio equilibrio interno".
Karl Von Clausewitz

Spinti dalle radio, dalla TV, o dal semplice passa parola, i social network stanno vivendo il loro momento magico. Che siano utili per tenere i contatti con gli amici, Facebook docet, o sistemi di contatto professionale, come LinkedIn, sembra che il mondo intero non ne possa fare a meno.

Per noi, che nel campo ci stiamo da anni non ci sono particolari novità: email, siti Web personali, bacheche elettroniche, chat e via dicendo fanno parte della nostra vita; la grande novità dei social network, è quella di mettere a disposizione nuovi strumenti di comunicazione alle persone comuni. La possibilità di fare ricerche in elenchi di iscritti andando a pescare vecchi amici di cui si sono perse le tracce, di vedere le loro foto attuali, di sentirli, di scambiare messaggi, sono tutti aspetti che portano con loro una elevata carica emozionale.

Bello, certo, ma allo stesso tempo i rischi a cui ci espone possono essere al di là del prevedibile: nel mondo reale, le emozioni positive e negative si depositano, permettendoci di assimilarle pian piano. I social network no: qui, come con qualsiasi cosa che abbia a che fare con i computer, tutto viaggia velocemente.

Quasi tutti i partecipanti di Facebook con amici nel Nord Italia hanno saputo del terremoto prima che l'ANSA battesse la notizia, in tempo reale. Così come hanno immediatamente avuto notizie di scioperi di treni, difficoltà dovute alle nevicate e così via. Questa velocità, applicata alle emozioni, può farci trovare impreparati di fronte a quello che ci avviene intorno, a ciò che capita al nostro gruppo di contatti.

A complicare le cose c'è anche il fatto questi nostri contatti non sono più limitati a quelli attuali, alle persone che fisicamente ci circondano, ma possono includere fantasmi dal nostro passato remoto: dalla ragazzina delle elementari di cui ci eravamo innamorati al collega che abbiamo avuto nel nostro primo lavoro, passando per tutta una serie di persone che abbiamo incrociato nella nostra vita.

L'unione della velocità con cui transitano le informazioni e del vasto numero di persone del nostro passato con cui, possiamo entrare in contatto può creare un'onda emozionale che ci trova impreparati generando le reazioni più diverse.

Il mondo dei social network è fantastico ma solo con la dovuta coscienza potremo apprezzarne i vantaggi minimizzando i problemi che potrebbe causarci.

Giga

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Malware Chart



KASPERSKY lab

Dopo scorso gennaio Kaspersky Lab ha reso pubbliche due singolari classifiche, che riportano i 20 malware più diffusi a livello mondiale. Si tratta di classifiche calcolate a partire dalle segnalazioni ricevute dai software Kaspersky installati in tutto il mondo, pertanto si basano su dati reali.

La prima è calcolata a partire dalle semplici segnalazioni, quindi valuta la diffusione in circolazione dei malware elencati, a prescindere che siano installati o no sul computer degli utenti. Dai dati presentati si notano due cose. Innanzitutto, spesso i malware usciti dalla classifica rientrano sotto altra denominazione (per esempio il worm AutoRun.eee.worm che si ripresenta come Worm.Win32.AutoRun.vnq); questo è dovuto in gran parte grazie alla natura automodificante con cui vengono programmati molti di questi programmi maligni. In secondo luogo, si ha una chiara idea di come siano suddivisi in percentuale le varie tipologie di software pericolosi: le tre macroclassi con cui Kaspersky classifica i programmi pericolosi sono Malware (15% delle segnalazioni), Trojware (i classici Trojan, 35%) e Virware (i virus propriamente detti, ben il 50%). In totale, Kaspersky Lab ha rilevato un totale di 46.014 malware in circolazione, dei quali ben 7.800 nuovi rispetto al mese di dicembre 2008 (in gran parte variazioni sul tema, cioè programmi automodificanti).

La seconda classifica è forse la più inquietante, in quanto si basa sull'effettiva presenza dei programmi indesiderati sul PC degli utenti, quindi va ad affinare i dati presentati dalla prima con quelli rilevati "sul campo". Da questa classifica si nota un incremento dei programmi classificati come virus veri e propri, cioè di quei programmi che sono in grado di infettare i file e non si limitano a installarsi nel computer come farebbe un trojan o uno spyware. Tra gli altri, si nota il nuovo ingresso di P2P-Worm.Win32.Deecee.a, un worm che si diffonde attraverso le reti peer to peer di DC++ rinominandosi dal suffisso "(CRACK)" o "(PATCH)" seguito dal nome di un programma famoso, come "ADOBE ILLUSTRATOR (All versions)" e così via.

1

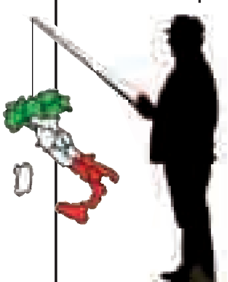
POSIZIONE	MODIFICA IN CLASSIFICA	PROGRAMMA MALIGNO
1	0	Virus.Win32.Sality.aa
2	0	Packed.Win32.Krap.b
3	1	Worm.Win32.AutoRun.dui
4	-1	Trojan-Downloader.Win32.VB.eql
5	3	Trojan.Win32.Autoit.ci
6	0	Trojan-Downloader.WMA.GetCodec.c
7	2	Packed.Win32.Black.a
8	-1	Virus.Win32.Alman.b
9	5	Trojan.Win32.Obfuscated.gen
10	10	Trojan-Downloader.WMA.GetCodec.r
11	Nuovo	Exploit.JS.Agent.aak
12	-1	Worm.Win32.Mabezat.b
13	-3	Worm.Win32.AutoIt.ar
14	1	Email-Worm.Win32.Brontok.q
15	Nuovo	Virus.Win32.Sality.z
16	Nuovo	Net-Worm.Win32.Kido.ih
17	Rientro	Trojan-Downloader.WMA.Wimad.n
18	-2	Virus.Win32.VB.bu
19	-2	Trojan.Win32.Agent.abt
20	Nuovo	Worm.Win32.AutoRun.vnq

2

POSIZIONE	MODIFICA IN CLASSIFICA	PROGRAMMA MALIGNO
1	0	Virus.Win32.Sality.aa
2	0	Worm.Win32.Mabezat.b
3	2	Net-Worm.Win32.Nimda
4	-1	Virus.Win32.Xorer.du
5	1	Virus.Win32.Alman.b
6	3	Virus.Win32.Sality.z
7	0	Virus.Win32.Parite.b
8	2	Virus.Win32.Virut.q
9	-5	Trojan-Downloader.HTML.Agent.ml
10	-2	Virus.Win32.Virut.n
11	1	Email-Worm.Win32.Runouce.b
12	1	Worm.Win32.Otwycal.g
13	1	P2P-Worm.Win32.Bacteraloh.h
14	4	Virus.Win32.Hidrag.a
15	5	Virus.Win32.Small.l
16	-5	Virus.Win32.Parite.a
17	Rientro	Worm.Win32.Fujack.bd
18	Nuovo	P2P-Worm.Win32.Deecee.a
19	-4	Trojan.Win32.Obfuscated.gen
20	Nuovo	Virus.Win32.Sality.y

ITALIA: CAMPIONI DI PHISHING

Per quanto riguarda la tecnologia, l'Italia di solito occupa gli ultimi posti delle classifiche mondiali. Meno male che c'è il phishing a tenere alto il nome del nostro Paese! Questi sono i dati emersi dal lungo documento redatto dal X-Force Trend and Risk Repor, il maggiore organismo di controllo per la pirateria mondiale. Nel 2008 l'Italia infatti è stata la seconda nazione al mondo per numero di organizzazioni criminali legate alle attività di phishing. Insomma, una gran parte delle mail (poste, banche, siti di e-commerce e altro ancora) che ci invitano a donare i nostri dati personali, provengono da computer italiani. I pirati nostrani stanno già lavorando per far sì che nel 2009 il titolo di Campioni del Mondo diventi finalmente nostro.



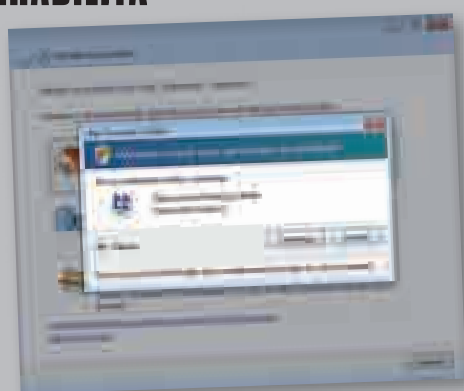
ASPETTA IL 23? NO, GOOGLE!

Google è il motore di ricerca più diffuso al mondo, eppure in alcuni Paesi in via di sviluppo, Internet rappresenta ancora un territorio sconosciuto a molti: tra questi c'è sicuramente l'India. Per avvicinare le persone all'utilizzo di Internet, e chiaramente per promuovere il portale, Google India ha tirato fuori un'idea davvero curiosa: un Google-bus che gira per le città e porta Internet agli utenti indiani. L'autobus, che chiaramente è personalizzato con i loghi di Google e la scritta "Explore the world of Internet", è dotato di alcune postazioni PC e schermi al plasma che permettono agli utenti indiani di sperimentare l'esperienza della Rete. La connettività è garantita dall'antenna satellitare che mantiene il collegamento a banda larga in tutte le 15 città toccate dal tour. Non sarà certo la soluzione a tutti i problemi del grande paese asiatico, ma l'iniziativa di Google è comunque da apprezzare.



WINDOWS 7: PRIME VULNERABILITÀ

La prima beta di Windows 7 aveva suscitato numerosi giudizi positivi tra gli addetti ai lavori. Avevamo parlato troppo presto! Molti utenti infatti hanno segnalato a Microsoft numerosi problemi di vulnerabilità dell'UAC (user access control) ovvero lo "scudo" che dovrebbe proteggere il registro del sistema operativo dall'installazione di software potenzialmente pericoloso per l'integrità di Windows. In pratica, per ovviare alle continue richieste di approvazione dell'UAC, Windows 7 integra una funzionalità automatica che automatizza alcune scelte sull'installazione del software proponendoci sempre meno spesso la classica "schermata grigia" dellUAC.



Un tentativo lodevole se non fosse che questa modalità può essere tranquillamente bypassata da alcuni software malevoli, aprendo di fatto le strade a virus e trojan. Microsoft ha comunicato di essere già al lavoro per rimuovere il problema e assicurare ai propri utenti la massima sicurezza e blah blah blah... come al solito.

TORNA LA VOCE AI VIDEO DI YOUTUBE

Nello scorso numero vi abbiamo dato notizia dell'accordo tra youtube e le major cinematografiche per mettere "il silenziatore" ai video protetti da copyright e pubblicati senza autorizzazione sul noto portale video. Bene, pare che il bavaglio durerà poco. La EFF (Electronic Frontier Foundation) infatti, ha deciso di dare supporto legale agli utenti che si ritengono danneggiati dal software che elimina l'audio, per intentare una causa contro youtube e affini. Infatti, l'avanzato sistema elettronico ha reso illeggibili anche numerosi video privati che nulla avevano a che fare con case discografiche o cinematografiche. La cosa interessante è che se la EFF vincerà la causa, tutti i video torneranno ad avere l'audio, in attesa di trovare un altro software più "preciso" in grado di bloccare solo quelli realmente protetti. Un'ottima notizia, davvero.



GOOGLE LATITUDE SA SEMPRE DOVE SIAMO!



Ecco un altro esempio di come si può limitare la nostra privacy con il pretesto di fornire un servizio allegro e divertente per tenersi in contatto con gli amici. Si chiama Latitude ed è prodotto (indovinate?) da Google! Il principio di Latitude è semplice: se abbiamo un cellulare compatibile con Google Maps 3, potremo creare una rete con i nostri amici per sapere sempre dove si trovano in qualsiasi momento. Latitude infatti sfrutta la combinazione tra GPS (nei modelli che ce l'hanno) e GSM per segnare la nostra posizione approssimativa su Google Maps. Lo stesso vale per i nostri amici: quando ci colleghiamo a Maps li vedremo sotto forma di "segnalini" sulla mappa della nostra città. Un ottimo modo per tenersi in contatto dice Google e per spiare mogli, fidanzate, amici, dipendenti e chi più ne ha più ne metta, aggiungiamo noi. Per fortuna in Italia il servizio non è ancora disponibile per ora!

NUOVO I PHONE DA APPLE?

Ci stavamo abituando adesso al nuovo iPhone 3g, con tutto il carico di novità ma anche di problemi che si porta dietro e voci di corridoio (nemmeno troppo fantasiose) ci dicono che Apple sta già pensando a una nuova versione del melafonino. A dare il via al gossip sono state le dichiarazioni (probabilmente scappate accidentalmente) del portavoce di una compagnia telefonica araba, che annunciava l'arrivo di un nuovo terminale della famiglia Apple per giugno di quest'anno. A dire il vero anche gli hacker del popolare DevTeam (coloro che hanno consentito lo sblocco a milioni di utenti) hanno trovato, nella lista dei dispositivi compatibili con il nuovo firmware, un misterioso iPhone 2.1 (il 3G è classificato come 1.2). Beh, nuovo telefono, nuovo sblocco da fare. Buon lavoro!



Oltre 90 mila violentatori su Myspace

I siti di social networking rappresentano una fantastica opportunità per tenersi in contatto con i propri amici nel mondo, tuttavia questi portali che consentono di fare amicizia con altre persone sono involontariamente un ottimo nascondiglio per criminali e malintenzionati. Il noto portale MySpace negli ultimi 2 anni ha individuato ed espulso ben 90.000 utenti condannati per violenza, grazie all'implementazione di un avanzato sistema di riconoscimento elettronico in grado di confrontare i dati inseriti dai "predatori" con quelli del database nazionale di "sex offender".



IL MULTITOUCH? ANDROID NON PUÒ!

L'arrivo del primo terminale smartphone dotato di sistema operativo Google Android (il famigerato G1) non è stato salutato da critica e utenti con quell'entusiasmo che Google si aspettava. Tra i motivi fondamentali di questo flop c'è sicuramente l'assenza del sistema di puntamento multitouch che invece ha decretato il successo planetario dell'iPhone di Apple. Secondo una fonte anonima che ha contattato il portale VentureBeat, il motivo della mancata implementazione di questa tecnologia sarebbero proprio gli accordi commerciali tra Apple e Google per lo sviluppo delle applicazioni per il suo iPhone. Apple, insomma, avrebbe vietato ai partner di Mountain View di utilizzare il multitouch per i propri telefonini, troncando di fatto le gambe all'interattività di Google Android. Quando si dice il mercato libero...



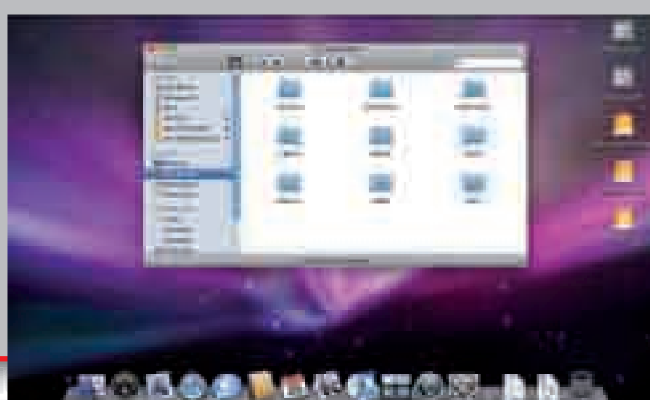
ECCO A VOI IL SESTO SENSO DIGITALE

Cos'è il sesto senso, quella particolare abilità di avvertire in anticipo un pericolo o di fare la scelta giusta al momento giusto? Per gli scienziati del MIT non è assolutamente nulla di "paranormale" ma più che altro la capacità, innata, di estrapolare informazioni aggiuntive dall'ambiente circostante che magari altri non riescono a inquadrare. Per dimostrare questa teoria, al MIT hanno costruito un dispositivo per ricreare un sesto senso "digitale" : si tratta di un sistema composto da una webcam, un mini proiettore e uno smartphone collegato alla rete. Una volta indossati questi oggetti infatti, gli utenti hanno la possibilità di interagire con il mondo esterno recuperando, tramite un complesso meccanismo di riconoscimento ottico degli oggetti, informazioni aggiuntive su quello che li circonda. Per esempio, se si sta guardando per strada la locandina di un film, il sistema recupererà il trailer e le eventuali recensioni, proiettandole sul primo muro disponibile: sarà quindi il "sesto senso" digitale a consigliarci se andarlo a vedere o meno. Inoltre la webcam è anche in grado anche di interpretare alcuni movimenti della mano per manipolare oggetti reali e virtuali dell'ambiente che ci circonda.



I CLONI MAC PARLANO TEDESCO

Va avanti la vicenda giudiziaria che vede Apple contro l'azienda tedesca Psystar rea di aver creato dei PC con installato il sistema operativo MAC OSX Leopard. Il giudice che presiede la causa, ha concesso l'autorizzazione a PsyStar per portare in tribunale le prove di alcuni vizi "burocratici" sul brevetto di MAC OSX che, per questo , non apparterrebbe di fatto ad Apple. Se quanto sostenuto da PsyStar fosse vero, per Apple sarebbero guai seri: l'azienda di Steve Jobs infatti perderebbe l'esclusiva su Leopard e nel giro di pochi mesi si potrebbero vedere in giro migliaia di "MAC Cloni" a prezzi più bassi e con hardware personalizzabili a dire il vero non siamo sicuri di parteggiare per Steve questa volta!

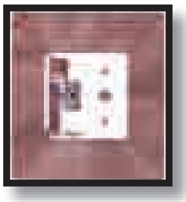




HOT NEWS

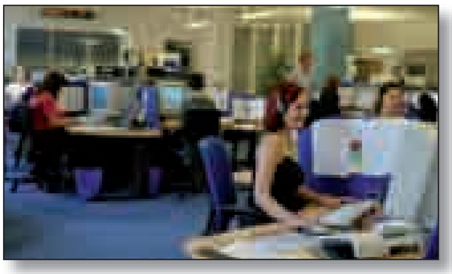
RFID, IL MODO MIGLIORE PER FARSI RUBARE I DATI

Lo hanno battezzato come "il codice a barre" del futuro e, negli USA, si sta progressivamente diffondendo in moltissimi negozi e supermercati, ma viene utilizzato anche dal governo per i passaporti elettronici. Parliamo chiaramente dell'RFID la tecnologia che permette di registrare informazioni (quali nome cognome, data, indirizzi, codici, e altro ancora) su un supporto delle dimensioni di un francobollo. Una rivoluzione nel campo della registrazione elettronica dei dati, se non fosse che… questi possono essere sottratti senza problemi con un lettore da 200 euro! La vulnerabilità è stata scoperta da Chris Paget, brillante informatico che ha sviluppato un sistema che aggira i sistemi di protezione dati integrati nel RFID e consente di recuperare le informazioni in esso contenute. La cosa più divertente è che la tecnologia wireless (alla base del progetto di questi chip) ha consentito a Chris di sottrarre dati da RFID distanti anche 40-50 metri. Una pacchia per i ladri di informazioni. Meglio i vecchi codici a barre per pane, latte e a cquisti vari e una bella foto sul passaporto per farci riconoscere.



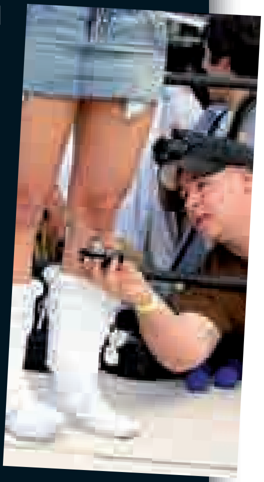
2009 ODISSEA NELLO SPAM

L'anno 2009 potrebbe essere ricordato come quello del telemarketing selvaggio e dello spam telefonico. Il Senato infatti, tra pochi giorni, dovrà trovarsi per decidere l'approvazione del cosiddetto decreto "milleproroghe" che sostituirà alcune leggi ormai vecchie relative alla garanzia per la privacy dei cittadini. All'interno del disegno di legge, è però presente un emendamento inserito bi-partisan dai senatori Fleres e Alicata (PDL) e Legnini (PD) che consentirebbe alle aziende di sfruttare gli elenchi telefonici pubblici precedenti al 2005 per svolgere attività di telemarketing fino al 31 dicembre 2009. Gli effetti di questo emendamento sarebbero devastanti in quanto autorizzerebbero qualunque società a telefonare a tappeto su tutto il territorio nazionale per reclamizzare "cornetta per cornetta" i suoi prodotti. Evidentemente i Senatori non hanno un telefono fisso a cui farsi chiamare…



BARO ON LINE

Aveva pensato a tutto l'impiegato di un ufficio pubblico di Albano Laziale: per appropriarsi di qualche immagine "hot" rubata nella toilette delle signore da guardare nella quiete casalinga, era bastato ricavare un piccolo spazio nel distributore delle salviette sufficiente ad inserire un telefonino dotato di videocamera collegato ad un hard disk esterno. L'hanno beccato! Ora rischia di passare un bel po' di tempo in galera con le accuse di interferenza illecita nella privacy e danneggiamento. L'hard disk, contenente le immagini incriminate è stato sequestrato (crediamo ben volentieri) dai carabinieri di Albano Laziale, per "ulteriori accertamenti". Morale: il voyerismo non paga!



I BLOGGER PAGATI DA GOOGLE

Se pensavate che la rete, e in particolare il blog, fosse uno strumento di libertà contrapposto alla TV che ci dice sempre le solite bugie, bene, probabilmente vi sbagliavate. Google infatti ha messo in atto un astuto, quanto inconfessabile tentativo per recuperare quote di mercato a Yahoo in un Paese altamente tecnologico come il Giappone: pagare i blogger per recensioni positive. Ebbene sì, di fronte allo strapotere di Yahoo sul mercato Nipponico, la divisione giapponese di Google ha deciso di "infiltrarsi" nelle pagine più cliccate attraverso un piccolo widget che riporta le parole chiave più cliccate quotidianamente. Per supportare questa iniziativa, che ha riscosso un buon successo, Google ha poi deciso di pagare alcuni blogger considerati "influenti" per scrivere recensioni positive sul widget e sul Google in generale in modo da orientare le scelte dei navigatori verso le pagine di "big G". Complimenti per la correttezza e non aggiungiamo altro.





ADOBE LIBERA TUTTI

Adobe pubblica le specifiche di Real-Time Messaging Protocol, usata in Flash Media Server ma non è tutto oro quel che luccica

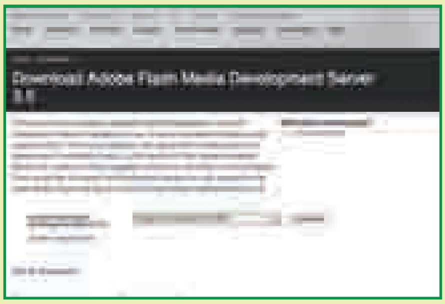
La notizia è di quelle destinate a scuotere la Rete, almeno quella parte della Rete che si occupa di video: Adobe ha deciso di rendere pubbliche, entro l'anno, le specifiche su cui si basa il Real-Time Messaging Protocol. Nato col nome di Flash Communication Server MX e sviluppato da Macromedia, è stato acquisito da Adobe insieme alla stessa Macromedia nel dicembre del 2005 ed è il sistema alla base dello streaming Flash che ha fatto il successo di molti siti tra cui il più noto è YouTube. Il protocollo RTMP, cuore del server, è stato finora proprietario, impedendo una libera concorrenza sulle piattaforme di streaming e creando una situazione di monopolio di fatto da parte della soluzione Flash.
La prima reazione è stata di entusiasmo: dal 2009 qualsiasi sviluppatore potrà creare programmi con tecnologia Flash incorporata senza dover pagare alcuna royalty ad Adobe. Questo darà modo agli sviluppatori indipendenti di entrare in un mercato promettente e agli sviluppatori di software Open Source di creare legalmente nuovi strumenti per le piattaforme più svariate. Basta però una piccola analisi per capire che Adobe sia stata costretta a compiere questo passo; i motivi sono diversi e c'è lo "zampino" di Redmond.



Adobe ha dichiarato che rilascerà entro l'anno le specifiche del suo protocollo RTMP ma non è certo un regalo: è indispensabile per la sopravvivenza di Flash.

:: Arriva Silverlight

Fino a qualche tempo fa lo status di monopolio di Adobe in questo mercato era indiscusso, Flash si era imposto facilmente grazie alle sue caratteristiche di leggerezza e qualità. Nel dicembre 2006, però, Microsoft rilasciò alla sua community di sviluppatori una pre release di un sistema, Silverlight, che doveva far concorrenza a quello che era già uno standard del Web.



Gli sviluppatori Adobe possono scaricare una versione dimostrativa gratuita del server di streaming ma devono comunque comprarsi gli strumenti di sviluppo.

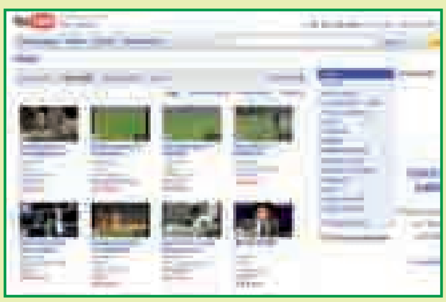
La prima versione pubblica (2007) non dava preoccupazioni: era lenta e usava una grande quantità di banda non ottimizzata. Dopo varie versioni però, venne rilasciata (2008) la versione 2 e tutto è cambiato. Silverlight si è dimostrato veloce, stabile e flessibile quanto Flash. Accanto alle novità tecniche, Microsoft ha lavorato sull'aspetto commerciale stringendo un accordo con Nokia per l'integrazione di Silverlight nei suoi telefoni, convertendo a SIlverlight tutti i propri siti e creando e fornendo gratuitamente agli sviluppatori. Net, un kit per la sua integrazione nei loro programmi. Proprio questa integrazione ha diffuso immediatamente il nuovo formato presso sviluppatori che non devono acquistare nulla per il suo utilizzo: è disponibile gratuitamente con gli strumenti di sviluppo che hanno già acquistato. Se, poi, non si ha acquistato nulla, si possono usare le versioni Express, scaricabili gratuitamente dal sito Microsoft. Un approccio ben diverso da Adobe che vende non solo le sue piattaforme server ma anche gli strumenti di sviluppo necessari.



Microsoft SIlverlight è il principale concorrente dello streaming di Adobe e sta diventando molto pericoloso: la sua diffusione è in netto aumento.

:: Flash ovunque

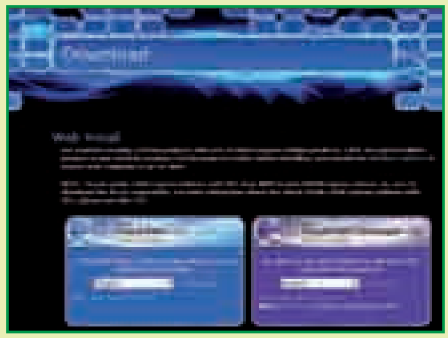
Ufficialmente, ovviamente, Adobe afferma che la sua decisione non è dovuta ad altro che al suo Open Screen Project: il progetto in corso da alcuni anni che ha lo scopo di rendere Flash lo standard di streaming disponibile con qualsiasi piattaforma: dal telefono al Web alla TV. Un'affermazione sicuramente vera visti gli sforzi di Adobe per creare player Flash adatti a qualsiasi piattaforma ma, anche un indizio di come l'uscita e il successo di Silverlight abbiano sostanzialmente sorpreso Adobe. Da questo punto di vista, l'approccio aperto che Microsoft ha con la sua community di sviluppatori ha permesso a Silverlight di superare immediatamente Flash grazie alla possibilità di passare alla nuova tecnologia a costo zero: senza cambiare strumenti di lavoro e con il pieno supporto da parte di Microsoft. L'unica carta che Adobe poteva giocarsi per recuperare il terreno perduto in questo progetto era proprio quella di rendere libere le specifiche e conquistarsi i programmatori dell'Open Source. La situazione, tuttavia, non è ancora in pareggio: la comunità di sviluppatori dovrà attivarsi per recuperare gli strumenti necessari all'integrazione di Flash nei loro prodotti. Dal punto di vista commerciale, invece, nessun team manager potrà più scegliere Flash a cuor leggero come piattaforma e sarà costretto a valutare attentamente anche Silverlight: esattamente la situazione che Adobe paventa ma che, fino a quando manterrà in vendita i suoi strumenti di sviluppo, non potrà modificare.



Youtube è sicuramente il sito più conosciuto che fa uso della tecnologia di streaming di Adobe per Flash.

:: Una rivelazione

A margine di questa notizia c'è da annotare una cosa importante: Adobe ha specificato che non verrà reso pubblico nulla di quanto riguarda le protezioni DRM usate dalla sua piattaforma di streaming perché una eventuale divulgazione le renderebbe vane.



SIlverlight gode di un vantaggio importante su Flash: se non si hanno strumenti di sviluppo, si possono scaricare gratis dal sito di Microsoft.

Un'affermazione, questa, che fa scalpore perché afferma intrinsecamente che l'applicazione del DRM nei filmati Flash non dipende da chiavi ma dallo stesso protocollo di cifratura utilizzato. È certamente un punto a sfavore di Adobe, visti i casi storici precedenti come quello del DES, in cui il reverse engineering ha distrutto completamente svariati sistemi di cifratura. Un'affermazione che gli esperti di crittografia vedono come l'indicazione che il sistema di cifratura e protezione usato da Flash è di tipo debole e potrebbe essere già compromesso.

IMMAGINI E MAPPE



Sfruttiamo un hack di Google Map per visualizzare sul Web immagini enormi

Internet come… blog. Internet come… e-mail. Internet come… post da inserire un po' ovunque. Tutti casi nei quali, spesso, dobbiamo allegare delle immagini. E se è vero che, con le connessioni veloci (almeno teoricamente) di cui disponiamo al giorno d'oggi, inviare un'immagine di grandi dimensioni è piuttosto veloce, è pur vero che la qualità delle foto digitali aumenta esponenzialmente. E dunque eccoci a preferire foto in bassa risoluzione, oppure "anteprime" che richiamano le versioni originali, in alta risoluzione. Insomma, il rapporto qualità/banda è rimasto più o meno il medesimo. La tecnologia software, per fortuna, si è evoluta, e consente di applicare alcuni trucchi niente male alle nostre foto, per mostrarle in tutta la loro grandezza e bellezza.

::Da Google in poi

È in particolare Google ad aver fatto passi da gigante in questo settore, e le sue Google Map ne sono la più chiara dimostrazione: mostrano mappe enormi, con una qualità così elevata da superare a pieni voti anche la "prova zoom". E, proprio basandosi sul lavoro di Google, il "Centre for Advanced Spatial Analysis" dell'University College London ha sviluppato un software in grado di rielaborare immagini di grandi dimensioni, per rendere "gestibili" direttamente dal web. Il suo segreto? Trasformarle in... mappe!



Il livello di zoom applicabile alle immense immagini è davvero impressionante.

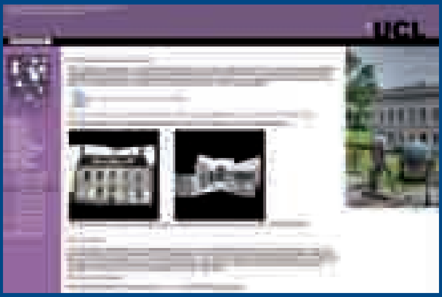
::Questione di tessere

Il principio su cui si basa Google Maps Image Cutter, questo il nome dell'applicazione, attinge a piene mani da quello delle Google Map, che a loro volta devono moltissimo a una tecnica molto in voga nei videogiochi degli anni '90: il "tiling". Questa tecnica, in buona sostanza, parte dal presupposto che un'immagine di grandi dimensioni occupa troppe risorse del sistema, se gestita interamente e in un sol colpo. Basti pensare che una foto di buona risoluzione arriva ad avere dimensioni anche di 10-15 mb: tranquillamente gestibili da un computer offline, ma davvero troppi se l'immagine è utilizzata o trasmessa online. Ecco dunque che l'immagine può essere suddivisa in tante "tessere" ("tile", da cui il nome della tecnica), di dimensioni e peso inferiori, da caricare solo all'occorrenza. Quindi, in buona sostanza, se zoomiamo su un'immagine e spostiamo la visuale sul suo angolo in basso a destra, sarà sufficiente caricare in memoria solo le tessere di quella porzione dell'immagine. Senza questa tecnica, sarebbe invece stato necessario caricare tutta l'immagine, e poi scorrerla fino al punto desiderato.

In realtà questa è solo una spiegazione di base, che riassume una tecnologia software molto complessa da progettare e realizzare. Fatto sta che Google Maps Image Cutter ha il pregio di renderla accessibile a tutti, applicando automaticamente il "tiling" alle nostre immagini. Dal punto di vista tecnico, l'algoritmo utilizzato, dopo il caricamento dell'immagine, si occupa di suddividerla in tessere da 256x256 pixel, mantenendo ovviamente la struttura originaria della foto. Fatto questo, genera un file per ogni tessera, e lo salva in un'apposita cartella. Infine, crea anche un file HTML che ha il compito di "ordinare" le tessere per ricostruire l'immagine originale, e renderla disponibile in un qualsiasi sito web. Il punto di forza di Google Maps Image Cutter, tecnologia a parte, è proprio quello di generare file compatibili con qualunque servizio web. E, dato che fa ampio uso delle API di Google Map, la compatibilità è garantita non solo con tutti i browser, ma anche con dispositivi mobili, come smartphone e telefonini.

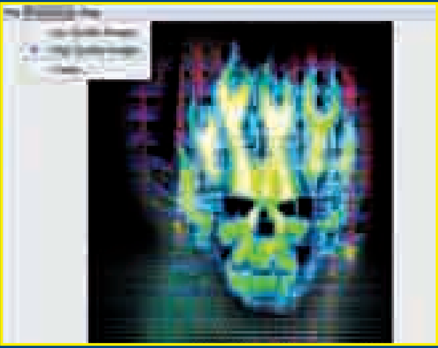
::Un software facile

Google Maps Image Cutter, insomma, va visto come un vero e proprio hack delle Google Map, inteso come metodo "alternativo" di sfruttare le potenti API messe a disposizione dal colosso americano. Andiamo quindi a dare un'occhiata a questa meraviglia; per prima cosa scarichiamola (gratuitamente) dal web: andiamo sul sito **http://www.casa.ucl.ac.uk/software/googlemapimagecutter.asp**, clicchiamo su Download versione 1.4 now, compiliamo il modulo e avviamo il download.



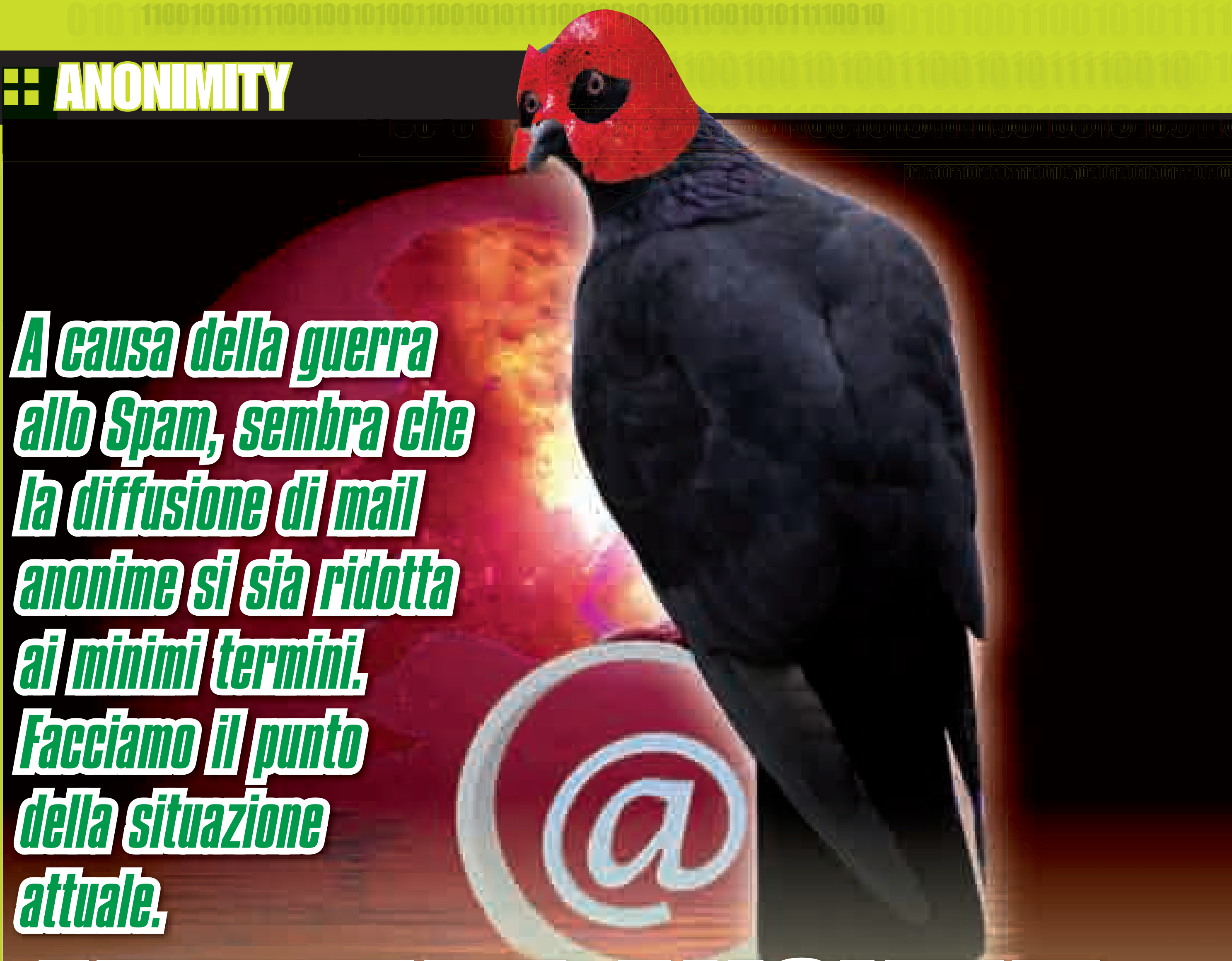
Il programma non gode di molti aggiornamenti, ma quel che c'è è già perfetto.

Fatto questo, estraiamo i file dell'archivio ZIP in una cartella qualsiasi del computer (meglio crearne una ad hoc), e facciamo doppio clic su GMapImageCutter.jar (per funzionare, il software richiede l'installazione del runtime java, scaricabile all'indirizzo http://www.java.com/it/download/index.jsp).Ci si presenta la schermata principale di Google Maps Image Cutter. Da qui, selezioniamo File/Open File e carichiamo l'immagine desiderata (di grandi dimensioni, senza paura di esagerare!) con un doppio clic. Il programma si occupa di suggerire un numero congruo di tessere, a destra, su Tile Count. Volendo, possiamo variarlo, agendo sul rispettivo cursore. Fatta la scelta, clicchiamo su Processing e selezioniamo il livello di qualità, tra Low Quality Images e High Quality Images.



L'interfaccia semplicissima: una sola funzione che si gestisce lavorando sulla barra a destra.

Il consiglio è di puntare al secondo, ma se il numero di tessere è molto elevato, diciamo superiore alle trentamila, e l'immagine molto grande, forse è meglio puntare alla bassa qualità. Infine, diamo il via ai lavori, cliccando su Create e poi su Start. A questo punto diventa tutta una questione di (dolce) attesa: in base alle scelte effettuate, la creazione delle tessere può richiedere da qualche secondo a un paio, o più, di ore. Al termine, Google Maps Image Cutter genera una cartella con le tile e il relativo file HTML. Per avere un'anteprima sul (capo)lavoro di questo software facciamo doppio clic proprio sul secondo, ed ecco che è visualizzata una "mappa" con l'immagine desiderata. A noi, ora, il piacere di scorrerla e zoomarci liberamente.



A causa della guerra allo Spam, sembra che la diffusione di mail anonime si sia ridotta ai minimi termini. Facciamo il punto della situazione attuale.

MITTENTI ANONIMI

Fino a qualche anno fa erano molto diffusi i programmi di mailing anonimo. Negli ultimi tempi, però, le cose sono cambiate. Hanno iniziato i grandi provider, seguiti a ruota dai piccoli, a impedire il relay della posta da domini esterni al proprio. Poi ci si sono messi molti governi nazionali, criminalizzando l'invio di mail anonime. Alla base di tutto è stata, purtroppo, l'aumento esponenziale dello SPAM che è avvenuto con incrementi record negli ultimi anni. A fronte di questa ondata di mail indesiderate, spesso impossibile da arginare a causa di cross-mailing tra operatori diversi, relay e sistemi anonimi, è stata data una risposta delle peggiori. Per prima cosa, per poter risalire all'IP del mittente e, spesso, alla sua identità, è stato instaurato il blocco del relay, costringendo gli utenti a continue modifiche del proprio server SMTP. Il secondo fronte, invece, ha riguardato la possibilità di inviare mail in modo anonimo, con l'addebito dello SPAM proveniente da un server al gestore del server stesso. Questa scelta, con l'inserimento dell'invio dello SPAM nei codici civili o penali della maggior parte dei paesi, ha obbligato la maggior parte dei creatori di server di uscita di mail anonime a chiudere i loro servizi. Nel caso in cui un server di questo genere facesse uscire messaggi di SPAM, infatti, il suo gestore potrebbe essere chiamato in tribunale a risponderne e sarebbe un suo

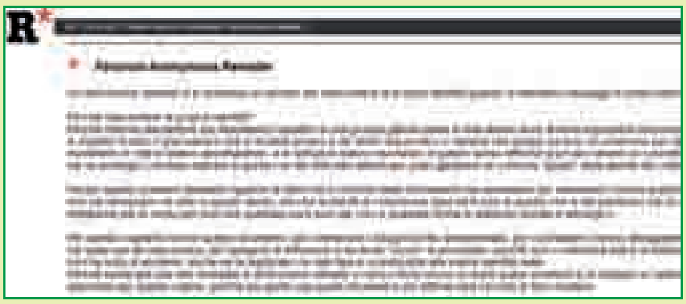


All'indirizzo isole.ecn.org/crypto/remailer/ si trovano le istruzioni per usare Cripto, remailer anonimo sostenuto dal progetto Winston Smith e dall'associazione Isole nella Rete.

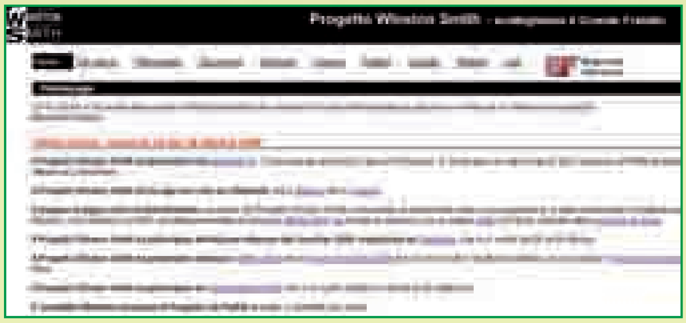
problema dimostrare che lo SPAM non è stato causato da lui ma da terzi.

:: Non tutto è perduto

A fronte di queste novità, portate avanti quasi parallelamente a livello globale, gli utenti di Internet si sono trovati su due fronti opposti. Un fronte, quello degli utenti di base, ha applaudito a queste iniziative che avrebbero dovuto stroncare lo SPAM. L'altro fronte, quello degli utenti evoluti, hanno visto in queste iniziative una serie di difficoltà poste all'invio di mail anonime. Oggi possiamo già concludere che queste iniziative sono state totalmente fallimentari: lo SPAM non è diminuito ma aumentato, in compenso moltissimi sistemi di mantenimento dell'anonimato hanno chiuso per sempre. Complessivamente, agli utenti meno smaliziati risulta oggi impossibile mandare mail anonime mentre gli spammers vanno avanti esattamente come prima, fatta salva qualche piccola condanna che ha coinvolto i più sprovveduti tra loro. Mantenere l'anonimato anche oggi, però, non è impossibile: è solo un po' più difficile che in passato. Di server che rendono anonime le nostre mail ce ne sono ancora. Quello che è sparito è il software, prima usato diffusamente, che permetteva l'uso di server anonimi in modo semplice. Attualmente, per esempio, esiste un solo programma di posta per Windows che supporta la cifratura per i sistemi di mailing anonimi: Sylpheed, sylpheed.sraoss.jp/en/. Di remailer anonimi, invece, ne esistono a livello mondiale circa una ventina, anche se il loro numero cambia in continuazione: mantenere un remailer anonimo può provocare problemi legali e non fa guadagnare assolutamente nulla. Uno dei remailer più usati in Italia è mantenuto dal Progetto Winston Smith, pws.winstonsmith.info. Si chiama Mixmaster.it e dispone di una pagina Web di aiuto all'indirizzo https://www.mixmaster.it.



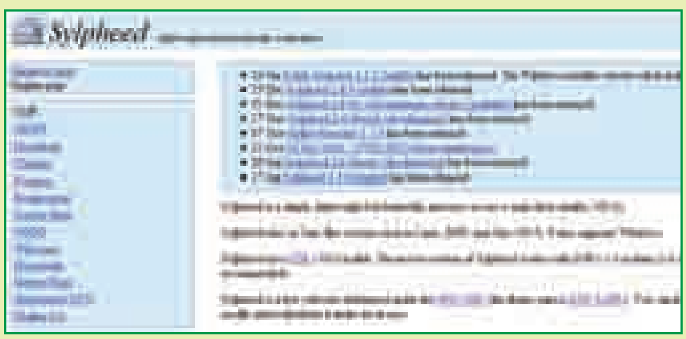
Il Collettivo Autistici/Inventati, http://www.autistici.org/it, fornisce diversi servizi veramente utili per mantenere l'anonimato navigando sul Web, tra cui un remailer di tipo mixmaster.



Il sito del progetto Winston Smith, pws.winstonsmith.info, contiene moltissime informazioni su come mantenere l'anonimato in Rete e proteggere la propria privacy.

:: Come funzionano

Il meccanismo di funzionamento di una comunicazione a un server remailer è abbastanza intuitivo, anche se non banale. Quando scriviamo un messaggio indirizzato a un remailer, inseriamo nella prima riga, per due volte, il simbolo dei due punti. Nella seconda riga scriviamo Anon-To:, seguito da uno spazio e dall'indirizzo del destinatario. Poi cifriamo il tutto usando la chiave pubblica del server a cui inviamo il messaggio. All'arrivo, il server decifrerà il messaggio, eliminerà le informazioni del mittente e provvederà a rispedirlo al destinatario indicato. Per ragioni di sicurezza è possibile inserire più trasferimenti da un server all'altro, in modo da rendere del tutto impossibile il recupero dell'identità del mittente. In questi casi basta ripetere i passaggi cifrando il messaggio cifrato. Prendiamo il messaggio già pronto per la spedizione al server che abbiamo scelto, inseriamo nuovamente per due volte il simbolo dei due punti sulla prima riga, mettiamo Anon-To: seguito dall'indirizzo del server di mailing anonimo a cui volevamo mandare il messaggio originale, cifriamo nuovamente il messaggio con PGP usando la chiave pubblica del nuovo server ed è fatto. Il messaggio ricevuto dal nuovo server verrà decifrato, reso anonimo e spedito al vecchio. Questo lo decifrerà, lo renderà nuovamente anonimo, rimuovendo i dati del passaggio dal server nuovo, e lo spedirà al destinatario.
Ripetendo l'operazione più volte creeremo una catena di server anonimi, spesso sparsi per l'intero pianeta, che renderà del tutto impossibile risalire alla nostra identità. Proprio per semplificare queste procedure, i server di mail anonimi si tengono in contatto periodico tra loro, in modo da creare liste di server anonimi che possono essere usate dagli utenti per creare la loro catena di server.



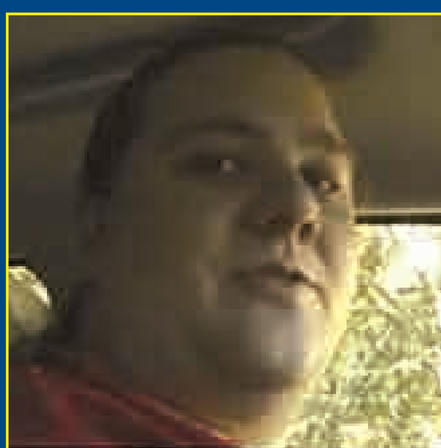
Sylpheed, che troviamo all'indirizzo sylpheed.sraoss.jp/en, è l'unico client di posta attualmente mantenuto aggiornato per l'uso con sistemi di remailing anonimi delle mail.



LADRI DI IDENTITÀ

Bastano 200 euro per appropriarsi dell'identità RFID di un ignaro viaggiatore

Quando sono stati presentati i primi dispositivi RFID siamo rimasti tutti meravigliati dal mondo di opportunità che questo sistema ci presenta. Dal semplice pagamento via cellulare compatibile, prima vera applicazione pratica del sistema, siamo passati ai documenti di identità rilevabili via radio; in particolare parliamo di patente e passaporto, come succede negli Stati di New York e Washington negli USA. Si tratta in effetti di tecnologie ancora in fase di sperimentazione (il passaporto in questione è limitato ai viaggi dei cittadini americani negli USA, in Canada, in Messico, ai Caraibi e nelle Bermuda), ma il governo degli Stati in questione incoraggia il passaggio e l'uso dei documenti RFID. Il guaio è che non si sta dando il giusto peso alle problematiche di sicurezza, come ha dimostrato e documentato il ricercatore informatico di San Francisco Chris Paget.



Chris Paget, il ricercatore americano che ha condotto questo studio sulla sicurezza dei documenti RFID, in azione.

:: In Aetheris Conjungo

Un dispositivo RFID è rilevabile mediante radiofrequenza e può trasmettere all'apparecchiatura adeguata diverse informazioni, dalle più semplici alle più sensibili: il numero dell'abbonamento al servizio di trasporto pubblico, il numero di carta di credito o i propri dati anagrafici. Il punto è disporre di questa apparecchiatura: siamo portati a pensare che sia altamente sofisticata e disponibile solamente per quegli enti ed esercizi che sono titolati per la sua gestione e il suo utilizzo, ma, come vedremo tra breve, non è così. Il fatto stesso che la comunicazione tra dispositivo e apparecchiatura avvenga via etere attraverso onde radio fa ben supporre che ci si possa piazzare nel mezzo con un ricevitore adeguato e impossessarsi delle



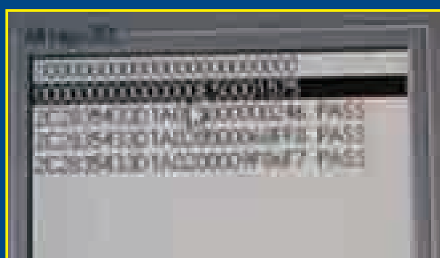
Gli stessi vetri oscurati nascondono l'antenna collegata al dispositivo, anch'essa trovata e comprata su eBay. Poca spesa, tanta resa.

informazioni che vengono passate. Chi commercializza questa tecnologia, in generale, si difende affermando che le portate sono talmente limitate che è praticamente impossibile intercettare le comunicazioni, a meno che l'oggetto dotato di sistema RFID non sia in mano nostra. Chris ha dimostrato il contrario: non solo è possibile aumentare tale portata, ma lo si può fare anche in maniera relativamente economica e con attrezzature facili da trovare e alla portata di tutti.

Questo la dice lunga sulla possibilità di usare questa tecnologia con la malizia di chi vuole spiare i fatti altrui, o peggio. "Il fatto che una cosa si possa fare", dice Chris, "non significa che la si debba fare per forza". Tuttavia noi cerchiamo di essere realisti e, così come lui ha condotto il suo studio, può esserci da qualche parte qualcuno che sfrutti la tecnologia malignamente a proprio vantaggio.

:: A caccia su eBay

Tutto ciò che è servito per condurre la ricerca è stato trovato su eBay, con una spesa complessiva che si aggira intorno ai 250 dollari (meno di 200 euro).



Il software scritto ad hoc da Chris, che ne renderà disponibili a breve i sorgenti, in funzione sul suo notebook Dell.

Ciò che gli serve è un ricevitore RFID con un'adeguata antenna, il tutto collegato a un computer su cui è in funzione un software scritto ad hoc. Il ricercatore ha montato questi dispositivi sulla propria auto, nascosti da sguardi indiscreti, e ha condotto il proprio studio guidando per le strade di San Francisco, ma nulla vieta a chi ha cattive intenzioni di escogitare altri stratagemmi. Per quanto riguarda la portata, Chris afferma che la sua installazione riesce a raggiungere i 12 metri, abbastanza per rilevare documenti RFID in tasca a chi passeggia accanto alla propria auto, ma dice anche che, con opportune modifiche, si può estendere il raggio d'azione fino a un miglio.



Il ricevitore RFID, comprato da Chris su eBay e usato per il suo esperimento, troneggia sul sedile posteriore del suo Volvo XC90 con vetri oscurati. Come un vero agente segreto.

:: I dati catturati

In realtà non sono stati rubati dati personali sensibili durante l'esperimento, pertanto l'identità delle "vittime" è protetta da anonimato. Ciò che è possibile captare con il suo sistema, infatti, è il codice identificativo univoco del chip RFID che è installato nei documenti di queste persone, e non i dati sensibili stessi. Tuttavia non è un dato da sottovalutare: con questo codice, infatti, si possono tracciare tutti i movimenti di una persona, arrivando a pedinarlo a livello di uno stalker accanito, ed è comunque il primo passo verso la clonazione dei suoi documenti. Con diverse tecniche di social engineering e appostamenti adeguati è possibile risalire agli altri dati, quelli più sensibili, ma senza questo codice non è possibile duplicare esattamente il documento. Come dire, ti clono il passaporto, vado all'estero a piazzare una bomba fingendomi te. A dir poco agghiacciante.

:: E le autorità nicchiano

Ciò che è più sconcertante non è tanto la possibilità che qualcuno si impossessi della nostra identità clonando un nostro documento RFID, quanto che le autorità fingano indifferenza e continuino a incentivare l'uso di questa tecnologia. I vantaggi che apporta, secondo le autorità statunitensi, sono maggiori dei rischi che comporta: più velocità nei controlli doganali e alle frontiere, per esempio.

Sicuramente lo spunto iniziale offre anche maggior sicurezza (è comunque più facile falsificare un documento cartaceo, per ora), ma se sono riusciti a creare apparecchi che clonano il Bancomat direttamente dallo sportello, quanto si crede che ci vorrà prima che qualcuno si crei il proprio passaporto elettronico falso?

ARRIVA LA BUROCRAZIA

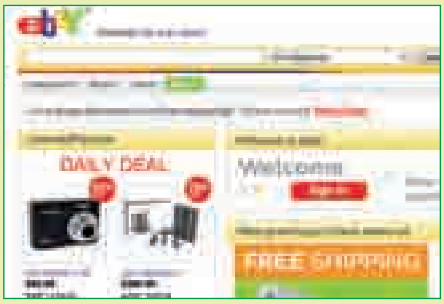


Comunicazione, velocità, essenzialità. Ma siamo proprio sicuri che le società della cosiddetta new economy siano proprio come crediamo?

La burocrazia sembra proprio essere una condanna dell'umanità. Una specie di castigo divino che, a un certo momento della storia di una società, inizia a dominarla completamente. Non ci stiamo riferendo allo Stato Italiano e nemmeno a qualche gigantesca società tradizionale ma alle società della cosiddetta new economy. Accumunate quasi tutte da una nascita spesso casuale, da intuizioni di ragazzi, cresciute nel corso degli anni mostrandosi innovative, moderne, veloci e amichevoli, negli ultimi tempi stanno iniziando a diventare le corporation tipiche degli incubi cyberpunk: burocratiche, enormi, lente, censorie e persino disumanizzate. Fino a quando si resta nei limiti indicati da queste società, come moduli di richiesta di informazioni o di segnalazione, tutto funziona a dovere. Funziona nel senso che sembra che i moduli arrivino veramente a destinazione. Per lo meno abbiamo l'idea che qualcuno abbia ricevuto le nostre comunicazioni anche se, magari, queste finiscono in una casella postale mai consultata. Se per una semplice segnalazione questo atteggiamento è valido, quando si tocca la sfera economica, le cose si complicano.

:: eBay piglia tutto

Nello specifico, attualmente, i maggiori problemi di questo tipo li sta soffrendo eBay. Nato come un piccolo sistema di vendita dell'usato, eBay è cresciuto sempre di più, affermandosi come un marchio internazionale di enorme valore. Col passare del tempo ha creato una piattaforma di vendita vincente, al punto da mettere in vendita qualsiasi cosa: letteralmente dallo spillo alla locomotiva. Naturalmente, come in tutte le società che si rispettino, la sua crescita non è dovuta solo al successo ma anche alle acquisizioni.

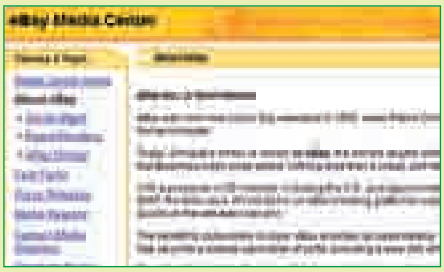


L'eBay originale, americano, si è evoluto da un'interfaccia semplice a una molto complessa, studiata per favorire in ogni modo la vendita dei prodotti.

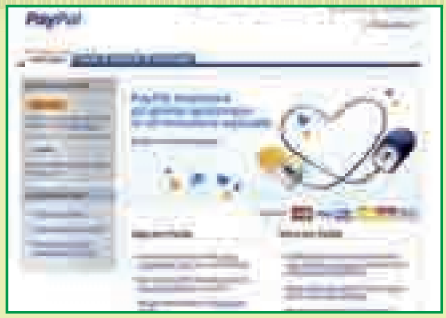
Da questo punto di vista, la decisione di comprare Paypal è stata quella forse più fortunata nella storia del commercio. Attualmente eBay gestisce ogni aspetto della vendita dei beni: dalla messa in vendita alla trattativa, dal pagamento alla gestione della reputazione dei venditori. Un sistema economico veloce, affidabile, ben conosciuto.
Con alcuni problemi, però, che si riflettono direttamente sui suoi utenti: truffe, merci di bassa qualità, copie pirata di CD e DVD, contraffazioni di oggetti di moda e via dicendo. A questi si deve aggiungere l'impossibilità di avere un contatto diretto con il sito stesso. È vero che si possono compilare moduli e segnalare le situazioni dannose per gli utenti, ma se si esce dagli schemi abituali delle vendite la situazione può diventare paradossale. Cosa succede se paghiamo un oggetto, ce ne viene recapitato un altro e il venditore si disiscrive dal sito? Cosa succede se abbiamo l'account di eBay bloccato e dobbiamo consultare informazioni dell'account per sbloccarlo? Oppure se cambiamo carta di credito qualche giorno dopo aver pagato con Paypal? Ad alcuni di questi quesiti eBay ha cercato di rispondere in vari modo ma nulla può fare per i migliaia di casi singoli, ognuno eccezionale a modo suo, che si verificano durante le transazioni.

:: Inumano

Per questi casi, in condizioni normali, si potrebbe ricorrere alle persone. A quello che, con linguaggio moderno, chiamo helpdesk: prendo il telefono e chiamo un assistente.



Le uniche informazioni pubbliche di eBay sono gli indirizzi postali delle sedi americane: decisamente poco utili per gli utenti italiani.



Paypal ha praticamente il monopolio dei pagamenti per conto terzi fatti sul Web: il blocco del suo conto, per molti, equivale al blocco del conto bancario.

Oppure gli mando una mail con tempi di risposta umanamente accettabili. Nella realtà, in nome della razionalizzazione del servizio e dell'abbattimento dei costi, questa condizione, nelle società della new economy, non si verifica quasi mai. Nel caso di eBay, poi, queste pratiche sono difficili da mettere in pratica: sul sito non vengono riportati indirizzi di posta elettronica ma solo moduli da compilare, con l'esclusione di quello riservato alle comunicazioni con le forze dell'ordine. Inoltre non c'è alcuna indicazione di numeri di telefono e nemmeno indirizzi di sedi fisiche della società in Italia o all'estero, con l'esclusione dell'indirizzo del quartier generale negli USA.

C'è un'unica informazione, reperibile tramite Google, ed è quella di una casella postale intestata a una banca milanese dove far pervenire i pagamenti delle commissioni. Per Paypal, le cose cambiano leggermente ma non di molto: è possibile contattare un operatore tramite telefono ma non ci sono riferimenti fisici a sedi italiane. Questo è, attualmente, il punto debole di tutta la catena ed è quello contro cui sono destinati a scontrarsi, prima o poi, tutti gli utenti: se seguiamo perfettamente il percorso previsto dal sito, facendo attenzione, eBay e Paypal ci daranno soddisfazioni. Uscendo minimamente dalle procedure previste, ci scontreremo con aziende assenti, latitanti e prive delle caratteristiche tipiche di un intermediario: la disponibilità di persone al servizio degli utenti.

STORIE DI VITA VISSUTA

Qualche tempo fa, ho effettuato l'acquisto di alcune foto digitali da usare per un sito su cui stavo lavorando, sul sito di un fotografo ed ho pagato con Paypal, senza alcun problema. Due settimane dopo ricevo diverse mail dal fotografo steso che mi chiede perché ho bloccato il pagamento e ho avviato la procedura di contestazione. Subito dopo ho ricevuto una mail da Paypal che mi richiedeva altre informazioni sul motivo della mia contestazione. Sono letteralmente cascato dalle nuvole e ci ho messo un po' a spiegare al fotografo che non avevo attivato alcuna procedura. Indagando un po' ho scoperto che il pagamento era stato fatto con la mia vecchia carta di credito che la settimana dopo è stata sostituita con una nuova. Avevo già aggiornato l'account di Paypal ma il pagamento era stato comunque fatto con la vecchia. Il risultato è stato quello di avere il blocco del pagamento e dell'account fino al termine della controversia. Sono seguite minacce di denuncia per infrazione del diritto d'autore da parte del fotografo, nuovo pagamento e successivo rimborso (sotto forma di nuove foto, e chi le voleva) una volta risolta la questione, e un o scambio infinito di mail. Un mese abbondante dedicato a risolvere una questione che una persona al telefono avrebbe potuto risolvere nel giro di qualche minuto.

Il PC ti riconosce

Con una libreria free possiamo dare al nostro PC capacità di riconoscimento ottico

La tecnologia avanza inesorabilmente e rapidamente, di questo ce ne rendiamo conto tutti i giorni; il bello è che ciò che un tempo era riservato a pochissimi iniziati e ai ricercatori, in grado di disporre di supercomputer e di fondi quasi illimitati, ora è sempre più a portata di tutti.



Ne è un esempio il tema di questo articolo: senza spendere un centesimo e con un po' di studio e di pazienza possiamo dare al nostro computer capacità ottiche. Non un semplice OCR, che riconosce i testi acquisiti via scanner, ma veri e propri occhi, in grado di rilevare e addirittura di riconoscere volti e movimenti.

:: Che cosa serve

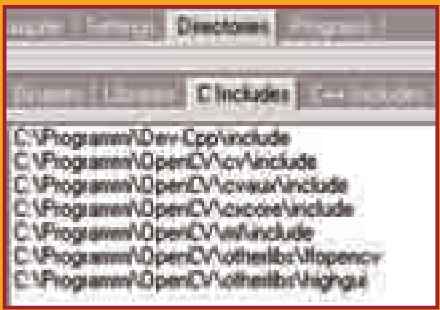
Per poter studiare questa affascinante branca della cibernetica, oltre al nostro fido computer (che, come sempre, più è pompato e più soddisfazioni ci darà) ci serve solo un compilatore C++ anche gratuito e OpenCV. Quest'ultima è una libreria sviluppata dal centro di ricerca Intel e ora liberamente disponibile come Open Source che può essere usata nei propri programmi, in unione a una periferica di acquisizione video (basta una semplice webcam), in grado di implementare quanto detto finora. La possiamo scaricare all'indirizzo http://opencv.willowgarage.com/wiki/Welcome, in cui troviamo anche esaurienti spiegazioni (in inglese) sul suo utilizzo e su come funziona.

Per quanto riguarda il compilatore, tanto dipende dal nostro sistema e dalle nostre possibilità. Se possiamo permetterci Microsoft Visual Studio tanto meglio, ma non è indispensabile: possiamo anche lavorare con la versione gratuita Express Edition oppure con un altro sistema di sviluppo, come Dev-C++ o Code::Blocks; dovremo però configurarlo adeguatamente per trovare e usare la libreria di OpenCV. Qui ci occuperemo di Windows con IDE gratuito, ma le informazioni di base valgono per tutte le eventualità.

:: Configurazione

OpenCV (l'ultima release è la 1.1pre1) è distribuita con un proprio installer che per impostazione predefinita copia tutti i file necessari nella cartella C:\Programmi\OpenCV; consigliamo di mantenere quella predefinita per facilità di gestione. In questa cartella troveremo librerie, documentazione e codice d'esempio. Prima di poter iniziare a lavorare con OpenCV dobbiamo però configurare l'IDE che useremo per programmare: in questo caso Dev-C++, ma con piccoli adattamenti si può procedere in maniera analoga anche con altri ambienti di sviluppo (facciamo sempre riferimento alle istruzioni sul sito). Una volta avviato Dev-C++, selezioniamo Tools/Compiler

Options per creare un nuovo profilo da usare quando compiliamo sorgenti che usano OpenCV. Nella finestra mostrata facciamo clic sul simbolo + e diamo un nome al profilo (OpenCV va benissimo).



Prima di usare OpenCV per scrivere i nostri programmi dobbiamo configurare l'ambiente di sviluppo perché riesca a trovare tutte le cartelle necessarie.

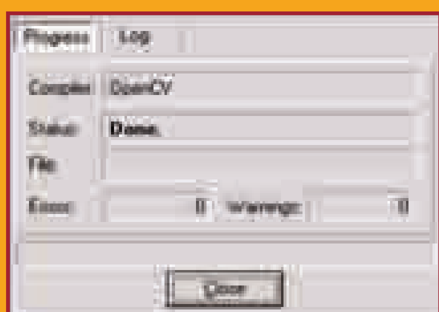
Attiviamo la seconda casella di testo (quella per le opzioni del linker) e inseriamo la stringa **-lhighgui -lcv -lcxcore -lcvaux**. Attiviamo quindi la scheda **Directories** e aggiungiamo, nell'ordine, **C:\Programmi\Dev-Cpp\lib\gcc\mingw32\3.4.2** e **C:\Programmi\OpenCV\bin** nella sezione **Binaries**, **C:\Programmi\OpenCV\lib** e **C:\Programmi\OpenCV\otherlibs\highgui** nella sezione **Libraries** e infine **C:\Programmi\OpenCV\cv\include**, **C:\Programmi\OpenCV\cvaux\include**, **C:\Programmi\OpenCV\cxcore\include**, **C:\Programmi\OpenCV\ml\include**, **C:\Programmi\OpenCV\otherlibs\ffopencv** e **C:\Programmi\OpenCV\otherlibs\highgui** nella sezione **C Includes** e nella sezione **C++ Includes**. A questo punto possiamo provare ad aprire uno dei programmi di esempio che troviamo nella cartella C:\Programmi\OpenCV\samples\c per vedere se la compilazione va a buon fine.

:: Come funziona

La libreria di OpenCV è costituita da cinque distinti elementi, ognuno preposto a determinate funzioni, che collaborano tra loro per dare il senso della vista al computer. CXCore è il cuore del sistema e contiene le strutture e gli algoritmi di base, nonché le funzioni per l'uso di XML e quelle per l'elaborazione grafica dei fotogrammi. Questi ultimi vengono forniti al core da HighGUI, la libreria che contiene le procedure di input/output per il sistema. CV è il segmento preposto all'analisi dei fotogrammi, quindi è il vero e proprio senso della vista della libreria.



La foto di gruppo mostra capacità e limiti di OpenCV: quasi tutti i volti vengono rilevati, fatta eccezione per quelli troppo in ombra, e vengono segnalati come volti anche altri elementi che evidentemente non lo sono. Si tratta dei cosiddetti "falsi positivi".



Se la configurazione è stata effettuata a dovere, provando a compilare uno dei programmi d'esempio dovremmo ottenere un messaggio di successo.

Alla catalogazione dei dati è preposta la sezione MLL, che comprende anche soluzioni di clustering per l'uso su PC multiprocessore. Oltre a questi è presente anche la sezione CvAux, che non fa parte direttamente del core del sistema ma che contiene varie linee di studio delle sue possibilità, come la visione stereoscopica o il tracking di oggetti nello spazio 3D.

:: Che cosa fa?

Le funzioni che OpenCV rende disponibili per gli sviluppatori permettono di compiere numerose operazioni su immagini e video, con particolare attenzione verso il riconoscimento dei pattern. Questo significa che possiamo usare sia immagini statiche sia immagini in movimento e istruire un nostro programma a riconoscere (con buone percentuali di successo) e a elaborare gli elementi che queste contengono. Per esempio, possiamo creare un programma che riconosca tutti i volti in una foto, li associ a un database contenente i nomi delle persone raffigurate e, ogni volta che viene rilevato un volto presente nel database, ci dia accesso alla scheda di quella persona. Oppure, possiamo approntare un software in grado di riconoscere determinati movimenti in un flusso video e intraprenda azioni diverse in base a quanto rilevato. Le applicazioni sono davvero molteplici e non hanno limiti, se non quelli della nostra fantasia.



LA TEMPESTA MUSICALE

Quando un problema di sicurezza si può trasformare in uno strumento di divertimento

Tempest è il termine che varie agenzie governative statunitensi (come la National Security Agency) usano per definire l'emissione di onde elettromagnetiche dai dispositivi elettrici ed elettronici, ormai diffusi in ogni ambiente. Anche le nostre case, circondati come siamo da aggeggi tecnologici di ogni genere, sono fonte ininterrotta di segnali radio spurii,. Su HJ 165 abbiamo già accennato al problema di sicurezza che questo può comportare: un malintenzionato dotato di una strumentazione adeguata può piazzarsi nella stanza accanto e intercettare ciò che scriviamo sulla tastiera. In realtà le cose sono ben più gravi, dato che non solo la tastiera è un'emittente di questo tipo di segnali radio; pensiamo, per esempio, al vecchio monitor CRT che ancora accompagna uno dei nostri PC: i segnali che trasmette possono permettere di ricostruire addirittura l'immagine mostrata.

:: Un po' di storia

La tecnica di intercettare i segnali RF spurii, denominata eavesdropping, ha origine nel corso della seconda Guerra Mondiale ed è stata rilevata dai laboratori Bell esaminando alcune parti elettroniche che fornivano all'esercito americano. Alla fine della guerra si è persa traccia di quanto scoperto, ma in seguito,, in epoca di Guerra Fredda, è tornato a essere oggetto di studi. Il primo documento ufficiale che riporta notizie interessanti è datato 1972 e spiega scoperte risalenti agli Anni '50, ma è stato rilasciato dalla NSA solamente nel 1997 (lo si può trovare all'indirizzo **http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf**).
In scenari degni delle migliori avventure di James Bond, varie agenzie di spionaggio e controspionaggio hanno individuato i



Lo smistatore crittografico Bell 131-B2, "colpevole" di trasmettere segnali spurii in grado di essere rilevati da un potenziale nemico, usato durante l'ultima Guerra Mondiale.

pericoli delle intercettazioni RF e hanno messo a punto delle contromisure; tuttavia ancora oggi i rischi di essere intercettati, benché fugati in ambito militare o di intelligence, sono tuttora presenti in ambito civile. È importante notare che il rischio di trasmissioni spurie non riguarda solo le onde radio, ma anche le linee di alimentazione: oggi usiamo la rete elettrica anche per portare Internet e comunicazioni via interfono e rete locale, ma la stessa è ricettacolo di scariche e segnali vari causati dal nostro PC e dagli altri apparecchi collegati.

:: Come difenderci

Oggi possiamo proteggere le nostre linee elettriche installando opportuni filtri e affidandoci a dispositivi adeguatamente schermati, ma questo limiterebbe la misura di sicurezza alle sole trasmissioni indesiderate che avvengono via cavo. Per i segnali captati via etere purtroppo si può fare molto poco: a parte cambiare il vecchio monitor CRT con uno a schermo piatto (che non è immune da problemi di trasmissione di questi segnali, ma lo è molto meno del fascio di elettroni di un CRT), la tecnologia non ci mette a disposizione molte scelte. Una di queste è l'uso di font opportunamente studiati per provocare emissioni talmente disturbate da non poter essere rilevate se non con molta difficoltà, o viceversa per ridurre al minimo le emissioni elettromagnetiche del monitor.

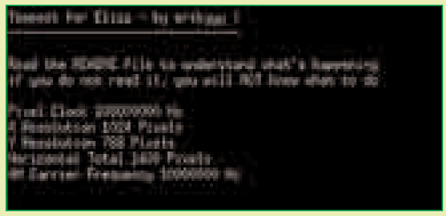
:: Divertiamoci con il problema

Sdrammatizziamo un po' quanto abbiamo detto: è molto difficile che qualcuno si armi di sofisticati dispositivi per venire a spiarci sotto casa e catturare le schermate del nostro monitor per vedere se guardiamo filmini porno. Anzi, possiamo usare questo problema per divertirci un po' con la nostra radio! Sfruttando la capacità del nostro vecchio monitor CRT di trasmettere segnali spurii, possiamo intuire che se lo pilotiamo adeguatamente le trasmissioni possono diventare intelligibili.



Un esperimento divertente: usiamo una radio AM per ricevere musica trasmessa dal vecchio monitor CRT!

Per esempio, usiamo una radio AM e, opportunamente sintonizzata, andiamo a ricevere musica trasmessa dal nostro monitor! Sul sito **http://www.erikyyy.de/tempest/** troviamo il lavoro svolto per noi da Erik Thiele. Il software Tempest for Eliza gira su Linux e, usando X, pilota il monitor CRT per trasmettere semplici brani simili alle suonerie di un cellulare. Non solo: una modifica al player permette di trasmettere anche i nostri file MP3; certo non ad alta qualità, ma comunque si tratta di un esperimento interessante. Sul sito troviamo i sorgenti per il programma, che possiamo compilare autonomamente (dobbiamo però disporre della libreria SDL, **http://www.libsdl.org/**). Se impostiamo la profondità di colore piuttosto bassa, come 8 bit per pixel, possiamo ottenere maggiore velocità e quindi migliore qualità di trasmissione.



Tempest for Eliza in funzione. Come suggerisce il testo, dobbiamo leggere il file README per capire cosa sta succedendo. I dati mostrati vanno annotati per comporre la nostra musichetta.

Per ricevere il segnale, dobbiamo usare una radio qualsiasi che abbia la capacità di sintonizzarsi sulle onde corte in modulazione di ampiezza (AM o SW secondo la radio). La frequenza ottimale si aggira intorno ai 10 MHz, dobbiamo sperimentare un poco per trovare la giusta sintonizzazione, che dipende dall'ambiente e dai dispositivi che usiamo.

:: Un piccolo aneddoto

Avevo recuperato da una BBS dedicata all'argomento un software per C64 in grado di ricevere (con una piccola basetta hardware da collegare al computer) le trasmissioni RTTY via etere e di decodificarle. Con un amico ho speso tutta la notte a cercare di sintonizzare la sua radio sulle giuste frequenze, e in effetti qualche carattere a caso appariva sul monitor. Alle 5 del mattino, dopo una notte infruttuosa, decidiamo che è ora di smettere. La radio era ancora sintonizzata su un segnale che ci pareva buono ma, spento il monitor, il segnale è scomparso. Una notte intera spesa a ricevere un segnale spurio del monitor che veniva tradotto in lettere a caso sul monitor stesso! Altro che tempesta...

I TRUCCHI DI VISTA



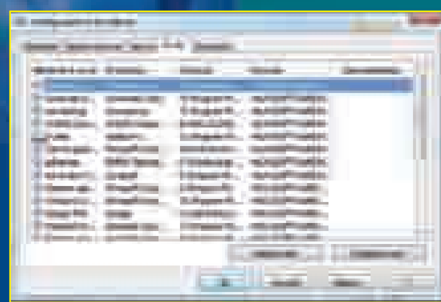
Programmi di avvio? "Killiamoli" senza patemi

I programmi dell'avvio automatico di Windows vengono eseguiti fin nei primi istanti di caricamento del sistema operativo, ma spesso il loro numero aumenta tanto da pregiudicare le prestazioni dell'SO. Senza contare che alcune applicazioni proprio non le vorremmo avviare: gli adware o spyware, per esempio, così mal programmati da non utilizzare nemmeno delle tecniche di stealth.

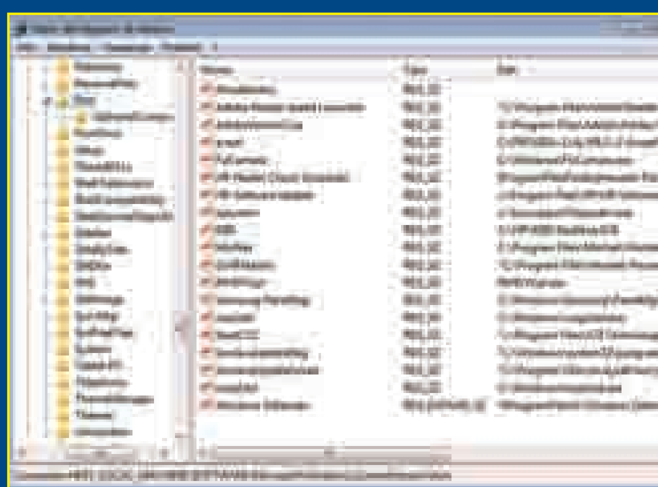
::La procedura

Il metodo più semplice per impedire l'avvio di questi programmi è quello di rimuoverli con il Pannello di controllo, ma a volte non figurano nell'elenco di quelli rimuovibili. Le alternative sono due: MsConfig e la modifica diretta del file di registro. MsConfig non è direttamente disponibile, pare quasi che Microsoft abbia voluto nasconderlo: selezioniamo **Start**, scriviamo **msconfig** nella casella di ricerca e premiamo **Invio**. In alcune configurazioni potrebbe essere presente il comando **Esegui**, come nel vecchio XP: basta quindi inserire **msconfig** nell'apposita casella e premere **Invio**. Facciamo quindi clic su **Continua**. Nella finestra del programma, apriamo la scheda **Avvio**. Ora, nell'elenco di applicazioni presenti, non ci resta che togliere il segno di spunta dalle caselle di quelle che vogliamo eliminare dall'avvio automatico. Infine, facciamo clic su **Applica** e poi su **OK**. Per rendere effettive le modifiche occorre riavviare il sistema. Per accedere direttamente al registro, invece, dobbiamo avviare RegEdit. Anche questo programma non è direttamente accessibile e dobbiamo comportarci come nel caso di MsConfig (scrivendo però **regedit**). Viene mostrata la struttura ad albero del registro: apriamo la chiave **HKEY_LOCAL_MACHINE**, poi **SOFTWARE**, **Microsoft**, **Windows**, **CurrentVersion** e infine **Run**.

È qui che spesso si nascondono programmi indesiderati che si avviano insieme a Windows. Va sottolineato che questa procedura non rimuove fisicamente un programma dal computer, ma solo il suo collegamento all'avvio automatico, così Windows non lo troverà. Ricordiamo però che disabilitare l'avvio di alcuni software dei quali non conosciamo la funzione può portare all'instabilità del sistema.



Qui troviamo tutte le applicazioni presenti nell'avvio automatico. Anche quelle che non compaiono nel Pannello di controllo.



Se usato male, RegEdit può compromettere il funzionamento del sistema operativo, quindi facciamo molta attenzione!

CREA IL TUO SITO DI
HACKER JOURNAL



Realizza il sito di Hacker Journal così come lo vorresti, pubblicalo in un area non indicizzata del tuo spazio Web e inviaci il link.

I migliori cinque, a insindacabile giudizio della redazione, verranno presentati nella home page di hackerjournal.it dove i lettori potranno votare ed eleggere il primo classificato.

Il sito vincitore verrà utilizzato, interamente, o esculsivamente come template grafica, come sito ufficiale di Hacker Journal.

Invia una mail all'indirizzo sito@hackerjournal.it con il link per visualizzarlo, i tuoi dati e una dichiarazione liberatoria di utilizzo.

www.hackerjournal.it

Tutti i segreti del tunneling

Come funziona la tecnica, molto diffusa, per aggirare firewall e filtri

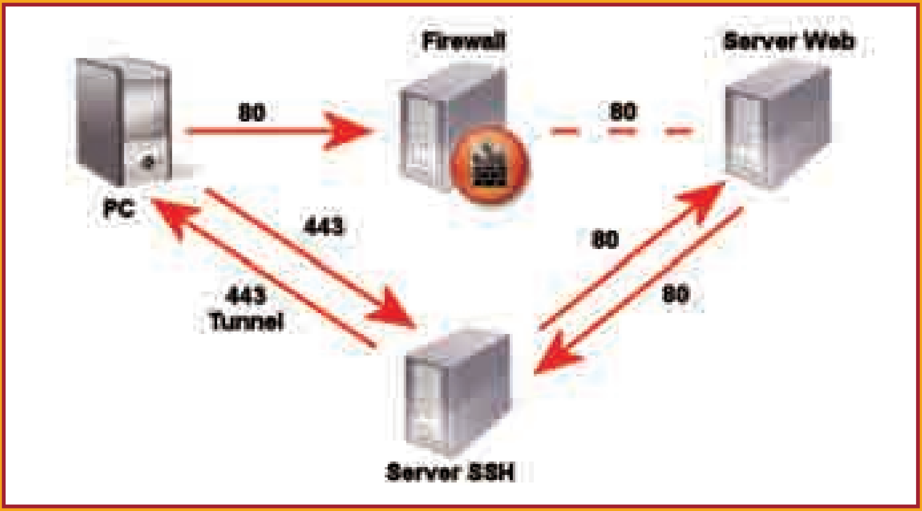
Il tunneling è una tecnica di instradamento del traffico via rete molto versatile e relativamente semplice da implementare, che comporta molti vantaggi. Tra questi, i principali sono una maggiore sicurezza delle nostre comunicazioni, che vengono crittate, e la possibilità di scavalcare eventuali filtri e impedimenti posti sulla rete che ci precludono l'uso di determinate applicazioni.

:: Il principio

Firewall e filtri di rete impediscono il traffico in entrata o in uscita su determinate porte o specifici indirizzi IP: per esempio, in un ufficio in cui i PC della rete non possono navigare sul Web. Si tratta di filtri che agiscono su canali ben precisi: per bloccare il traffico sul Web basta impedire l'accesso alla porta 80 a tutti i PC non autorizzati. Se però è possibile raggiungere almeno un computer con accesso libero a Internet (e noi abbiamo accesso a questo computer, perché per esempio si trova a casa nostra), possiamo sfruttarlo, trasformandolo in un server proxy nascosto, per navigare a dispetto di tutte le limitazioni. Un trucco vecchio come i firewall stessi. In più la comunicazione risulta crittata, quindi nessuno sarà in grado di osservare cosa stiamo facendo.

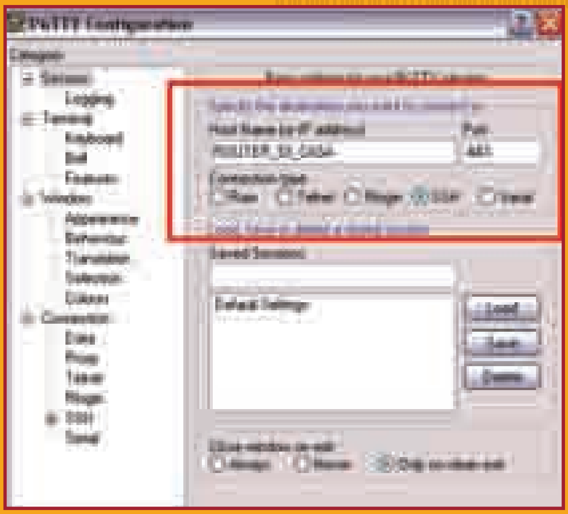
:: Un esempio pratico

Implementare un proxy privato per avere una via di uscita, un tunnel, è più facile in Linux che in Windows, ma anche in quest'ultimo non è impossibile.



Lo schema di principio del funzionamento di un tunnel SSH. Adottando un sistema come questo nessun firewall può fermare le nostre comunicazioni.

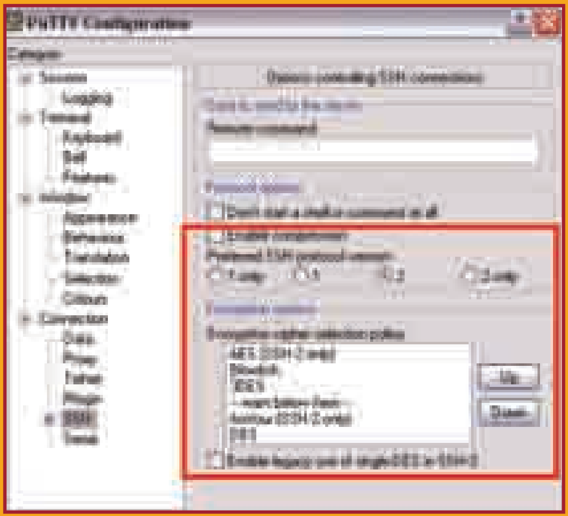
In Linux, gli strumenti necessari sono due: Privoxy e ssh (questo già presente normalmente nel sistema operativo). Privoxy è disponibile per varie distribuzioni e in codice. Quando è installato correttamente, Privoxy si aggancia per impostazione predefinita alla porta 127.0.0.1:8118, pertanto accetta connessioni solo da localhost. Sul server è tutto ciò che dobbiamo fare. Sul nostro computer invece i passi sono due: prima attiviamo il tunnel SSH impartendo il comando **ssh -NL 8118:localhost:8118 user@server** (questo comando crea il collegamento crittato tra la porta 8118 del nostro computer e la porta 8118 del server su cui gira Privoxy), poi configuriamo il browser per usare come proxy server localhost e come porta la 8118. In questo modo le comunicazioni che avranno luogo su tale porta verranno automaticamente trasferite sulla corrispondente porta del server, il quale recupera la pagina Web desiderata e la ritrasmette mediante la medesima connessione in tunneling al nostro browser.



Il primo passo della configurazione di PuTTY, che deve essere installato sul PC che usiamo in ufficio.

:: E in Windows?

In Windows è necessario qualche passaggio in più, perché non dispone di suo del comando ssh e quindi dovremo procurarci un suo sostituto. Scarichiamo l'ultima release di OpenSSH (http://sourceforge.net/projects/sshwindows/). Immaginiamo quindi questo scenario: siamo in ufficio, vogliamo dare un'occhiata a cosa succede su Facebook ma l'amministrazione dell'azienda non lo permette in orario di lavoro. Bene, la sera prima installiamo OpenSSH sul computer di casa e configuriamolo seguendo la documentazione fornita. Nel file di configurazione poi rimuoviamo il commento dalla riga dedicata alla porta da usare e cambiamola con la porta 443, dedicata al protocollo HTTPS. In questo modo eviteremo anche che il nostro tentativo di tunneling venga rilevato da software appositi che potrebbero girare in azienda. Rimuoviamo il commento anche dalla linea AllowTcpForwarding e impostiamola a Yes. Ora dobbiamo configurare il router di casa perché trasmetta via NAT o Port Forwarding il traffico sulla porta 443 verso il nostro PC: seguiamo le istruzioni dedicate al modello in nostro possesso. Scarichiamo quindi PuTTY (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) e salviamolo su una chiavetta Usb. Come ultima cosa, per poter accedere al router di casa dall'esterno dobbiamo conoscerne l'indirizzo IP.



La configurazione del sistema di crittografia da usare in PuTTY. Con questo accorgimento ogni nostra comunicazione sarà al sicuro da sguardi indiscreti.

Se abbiamo un abbonamento con IP fisso questo non è un problema, ma la maggior parte di noi avrà un abbonamento con IP dinamico. Possiamo risolvere questo problema sfruttando un servizio come DynDNS o simili.

Sul computer dell'ufficio dobbiamo installare PuTTY e configurarlo adeguatamente. Nella scheda Session impostiamo l'IP del router di casa, la porta 443 e attiviamo il protocollo SSH. In Connessioni/Proxy dobbiamo impostare il proxy usato. Se la rete aziendale è configurata per usarne uno dobbiamo rilevarlo dalle impostazioni del browser e riportarle in PuTTY, altrimenti possiamo lasciare HTTP. Infine, in SSH assicuriamoci che sia selezionato il tipo 2 e che AES risulti come primo metodo di cifratura nella casella in basso (se non è così portiamolo su noi). Ora viene la parte difficile: in SSH/Tunnels, impostiamo Source port con il numero di porta sul computer dell'ufficio che vogliamo forwardare (ad esempio 80 per poter navigare in santa pace). In Destination inseriamo localhost:443, così il router a casa saprà a chi dovrà reindirizzare la comunicazione. Facendo quindi clic su Open dovrebbe aprirsi la connessione verso il PC di casa attraverso il tunnel. Dobbiamo quindi configurare il browser per usare come proxy localhost:443 e a questo punto nessun filtro imposto dall'azienda potrà impedirci di fare un giro su Facebook.

:: Altri scenari

Impostando il tipo di proxy su SOCKS4 o su SOCKS5 possiamo usare questa tecnica anche per applicazioni che normalmente non prevedono l'uso di un server proxy, come un istant messenger o un programma per IRC. Questo ci apre un intero mondo di possibilità, contemporaneamente garantendo la sicurezza delle comunicazioni grazie alla crittografia applicata alle stesse. Buon divertimento!

ICE ATTACK

Una tecnica di attacco che sfrutta un problema hardware che non ha ancora rimedio

Siamo sicuri di aver reso il nostro PC una vera e propria cassaforte inespugnabile: abbiamo imposto password di accesso ovunque possibile e usiamo Truecrypt per mettere al sicuro i dati. Abbandoniamo il PC per andare in pausa pranzo, stiamo via un'oretta e al ritorno scopriamo che le nostre password sono state usate per rubare informazioni sensibili che riguardano le operazioni della nostra azienda. Ma come è stato possibile se avevamo preso tutte le precauzioni?

:: Dove finiscono le password

Quando proteggiamo il computer con i sistemi elencati, usiamo diverse password che fungono spesso da chiavi crittografiche con cui il software di turno recupera i dati. Dato che queste password le usiamo solitamente una volta sola, è logico pensare che i programmi di crittografia la immagazzinino in qualche maniera, per non costringerci a inserirla per decrittare ogni singolo frammento di informazione. Se la password fosse salvata su disco verrebbe meno tutto il sistema di sicurezza, pertanto viene immagazzinata solo nella memoria RAM e usata finché necessario. Allo spegnimento del PC la memoria viene azzerata, quindi la password e i nostri dati sono al sicuro. Questo è il nostro parere.



:: Come funziona la RAM

La memoria RAM del PC è definita di tipo volatile perché, per poter mantenere immagazzinati i dati, deve essere continuamente "rinfrescata". Questo significa che, a cadenze regolari, la circuiteria del modulo invia a ogni chip un segnale che lo costringe a ridare alimentazione alla cella di memoria, mantenendola attiva con il suo contenuto corrente. Nel momento in cui manca l'alimentazione, il contenuto della cella degrada progressivamente, fino al punto in cui non è più possibile leggerlo.
Questo tempo di decadimento varia in base a diversi parametri, come il modello e le caratteristiche dei chip di memoria e la temperatura ambiente, e può variare da pochi istanti a diverse decine di secondi in condizioni normali. Più è bassa la temperatura, maggiore è il tempo necessario perché il contenuto di un modulo di memoria RAM degeneri fino a diventare illeggibile.



Confronto d'esempio tra quanto contenuto in una memoria RAM al momento in cui viene spenta e quanto è possibile leggere dopo un certo tempo. Dopo 40 secondi l'immagine è ancora riconoscibile.

:: Cold boot attack

Sfruttando questo tempo di latenza tra lo spegnimento del PC e il decadimento delle informazioni, è possibile recuperare il contenuto della RAM direttamente, senza passare dal sistema operativo. I metodi utilizzabili sono diversi e dipendono dal tipo di computer sotto attacco, ma la cosa importante è che l'attaccante deve avere accesso fisico al PC (rubando un notebook, o accedendo fisicamente alla nostra stazione di lavoro). Sostanzialmente può agire in due modi: il primo prevede l'estrazione del modulo di memoria dal PC, il secondo l'accesso ai file creati dal sistema per salvare il contenuto della RAM per un rapido riavvio.

:: Memoria a freddo

Trovando un PC acceso, il cracker si comporta in questa maniera. Per prima cosa apre il case del computer e spruzza con una comune bomboletta di aria compressa sui moduli di memoria (questo permette di raggiungere temperature bassissime, intorno ai -50° C). Estrae quindi i moduli e li inserisce in un secondo PC o in un dispositivo apposito, programmato per fare il dump diretto della memoria su un'unità a disco o una chiave USB al momento dell'accensione. Può quindi reinstallare i moduli nel primo PC e portarsi dietro il dump, che esaminerà con calma per estrapolarne le password eventualmente contenute.

In certi casi non è nemmeno indispensabile estrarre fisicamente i moduli di memoria: se il PC può essere impostato per effettuare il boot da un'unità esterna come una chiavetta USB, al riavvio la prima cosa che questa chiavetta farà è copiare il contenuto della RAM sfruttando il tempo di latenza maggiore dato dal soffio di aria fredda. Da questo tipo di attacco possiamo difenderci impostando una password di avvio al boot del PC, che risiede nel BIOS e non in memoria, e disabilitando l'avvio del PC da unità esterne; ma nel caso vengano smontati i moduli di memoria c'è ben poco che possiamo fare.



Portando la temperatura della memoria parecchi gradi sotto lo zero, anche con una comune bomboletta di aria compressa, il contenuto viene preservato anche oltre i 10 minuti. l'immagine è ancora riconoscibile.

:: Dormienti e fregati

Sfruttando lo stesso problema dello spegnimento brutale e del riavvio da un'unità esterna, il malintenzionato può rubare gli eventuali file che il PC crea quando lo si pone in stand-by e studiarli con calma. Trovandosi davanti a un PC acceso, può forzarne la modalità stand-by, spegnerlo brutalmente e riavviarlo dalla propria chiavetta USB copiando i file contenenti il dump della memoria direttamente dal file system del computer. Nei computer più recenti è disponibile una modalità alternativa più sicura.



Sfruttando il boot da unità esterna e appositi software un cracker può effettuare il dump della memoria subito dopo il riavvio e rubare anche le password di Windows e di Truecrypt.

Selezionando la modalità ibernazione quando dobbiamo allontanarci dal PC, tutte le password crittografiche vengono tralasciate ed eliminate creando i file di ibernazione (che sono in effetti dump della memoria RAM), pertanto anche rubando questi file un cracker non potrebbe risalire alle nostre password.

:: Senza soluzione

Questo problema, come abbiamo visto, è dovuto a una caratteristica fisica dei moduli di memoria RAM: non sono possibili quindi adeguate contromisure definitive. Nel corso degli anni il progresso tecnologico ha creato moduli con tempi di latenza sempre più brevi, ma un cracker attrezzato può porre rimedio a questo intoppo sfruttando azoto liquido, che porta la temperatura fino a -197° C e un tempo di latenza di oltre sei ore. Queste tecniche vengono usate anche in ambito forense da parte delle forze dell'ordine, in occasione dei sequestri di materiale informatico.

Mela fai-da-te



Mettiamo l'ultimo Sistema Operativo Apple su un PC a basso costo

Recentemente è stato lanciato sul mercato un sub-notebook della Micro-Star (MSI) chiamato Wind PC. Ora è uscita la versione desktop che incorpora molti dei vantaggi di una tecnologia compatta, silenziosa e dai bassi consumi dei notebook: occupa poco spazio ed è abbastanza elegante da lasciarsi guardare in ogni ambiente. Ma ha soprattutto due caratteristiche interessanti: ha un costo molto basso e il suo hardware è compatibile con Mac-OS X.

:: Cosa ci occorre

Negli Stati Uniti è possibile prenderlo con 140$ e una licenza di XP, qui purtroppo si spende più del doppio per avere la versione base con linux a bordo. Nella confezione troviamo uno chassis nero dotato di un processore 1.6GHz Intel atom, un hard-disk SATA da 160Gb, un lettore dvd Super-Multi. È dotato di una scheda di rete ethernet da 1Gb e, per chi ha qualche euro in più da spendere la connessione wi-fi e il lettore di card reader 4-in-uno.
La tastiera dei notebook privi di tastierino numerico e soprattutto il mouse pad non sono il massimo della praticità, se pensiamo di usarlo come computer principale meglio pensare ad aggiungere tastiera e il mouse. Ultimo, ma non ultimo un buon monitor.

Oltre al Wind PC ci occorre il software. Se vogliamo fare una prova a scopo didattico, prima di procedere ad acquistare la nostra copia originale di Leopard, possiamo fare un giro su Internet per trovare il torrent di MSIWindosx86.iso. Ovviamente ricordiamo a tutti che scaricare e conservare tale iso è illegale se non si possiede anche una regolare licenza e anche in questo caso va considerata solo come copia di riserva.

Dati i collegamenti SATA non è possibile utilizzare vecchie periferiche ATA a meno che non si abbia un adattatore (se ne trovano anche su eBay). Se il bios è già aggiornato alla versione 1.50 o successive (visibile premendo CANC al boot del pc) possiamo procedere con l'installazione del nostro nuovo sistema operativo: Leopard.

Avremo bisogno di:
- 1 dvd vergine
- una penna Usb (solo se dobbiamo aggiornare il bios)
- un altro PC in grado di masterizzare i dischi

Se ancora non abbiamo il nostro Leopard originale, masterizziamo sul PC la ISO (consiglio di farlo a velocità 2X).

:: Assemblaggio

Se stiamo masterizzando, nell'attesa possiamo procedere con l'assemblaggio del Wind PC (che di norma dovrebbe essere fornito smontato). Va rimosso il coperchio superiore (ci sono due viti nella parte superiore del



Ecco come si presenta il case una volta che abbiamo tolti gli imballi.



Solo dopo aver tolto il coperchio possiamo accedere alla struttura interna.

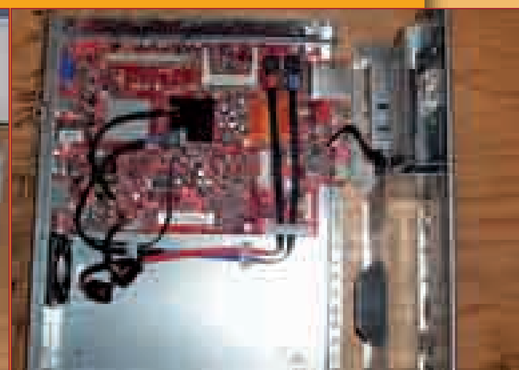
retro del case) facendolo scorrere. Poi va rimossa la mascherina frontale. Ci sono altre due viti che tengono il cestello del dvd montato che vanno tolte, dopodiché si possono inserire i drive all'interno. Chiaramente nel caso in cui usiamo un dvd ata con adattatore, conviene lasciare tutto smontato finché non abbiamo finito l'installazione di Leopard, altrimenti possiamo riassemblare il cestello. Ora si può inserire l'hard-disk, collegare le alimentazioni e rimontare la mascherina frontale. Prima di rimettere il coperchio procediamo con l'installazione della ram, da inserire con un angolo inclinato.

:: BIOS upgrade

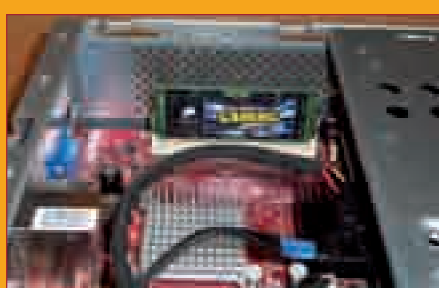
Se abbiamo già un firmware uguale o superiore alla 1.50 possiamo passare allo step successivo, altrimenti installiamo la utility HP format (che possiamo scaricare all'indirizzo www.hwsetup.it/hwsfiles?action=download&file_id=2138) e prendiamo la penna usb. Scarichiamo e installiamo il tool sul PC (non sulla penna), decomprimiamo i file di boot di Windows98 (lo troviamo all'indirizzo files.extremeoverclocking.com/file.php?f=196), dopodiché lanciamo HP format. Selezioniamo prima i file di Win98 e quindi il formato con cui formattare la penna Usb (Fat o Fat32 vanno bene entrambi). Una volta che la penna è pronta, decomprimiamoci dentro anche il Wind bios update (www.uselessninjas.com/downloads/msiwindosx/biosflash/biosflash.zip). A questo punto inseriamo la penna nel Wind PC e premiamo F9-F12 durante il boot. Selezioniamo quindi la penna Usb e vedremo partire il boot di Windows98. Una volta completato, dal prompt digitiamo flash.bat e premiamo Enter. Incrociamo le dita sperando che non ci siano problemi (un ups sarebbe sempre consigliabile per evitare sorprese legate ai cali di tensione) e avremo il bios aggiornato. A questo punto togliamo la penna e riavviamo, ottenendo un check-sum error al boot (tranquilli è tutto regolare: si può ignorare con F2).



Il rack drive va rimosso per poterci installare il lettore dvd.



Rimuovendo il rack si possono installare sia l'hard-disk che la ram.



L'inserimento di un banco ram è un'operazione semplice, alla portata di tutti ma va sempre fatta con attenzione.

:: Installazione

Nel bios settiamo le porte Usb da 480mbps a 12mbps e premiamo F10 per salvare ed eseguire un Restart. Premiamo F9-F12 e selezioniamo il drive dvd dove avremo inserito Leopard avviabile. Quando richiesto partizioneremo l'hard-disk (consigliato Mac OS journaled) etichettandolo con il nome che ci piace di più, Leopard ad esempio e diamo conferma.

Proseguiamo con l'installazione indicando la partizione appena creata e prima dell'Install vero e proprio selezioniamo Customize e deselezioniamo Patches->Kernel. Ora può partire l'installazione vera e propria che durerà circa 30 minuti, dopodiché si riavvierà il PC.

:: Primo boot

Il nostro Wind PC si riavvierà mostrando il bootloader di Leopard e potremo goderci il count-down aspettando che faccia il primo avvio (lasciare ancora il dvd inserito). A questo punto andremo a inserire i dati utente e una volta arrivati al desktop dovremo riavviare la rete per avere la ethernet funzionante.

Tornati al desktop, va dovremo compiere l'ultima operazione, ossia decomprimere il GMA950 package che contiene i driver video (li troviamo all'indirizzo www.uselessninjas.com/downloads/msiwindosx/GMA950.pkg.zip). Un ultimo riavvio e finalmente il nostro clone-Mac fatto in casa sarà pronto per funzionare.

ALL IN ONE

Come trasformare il nostro amato telefonino in un telecomando universale



Lo portiamo con noi tutto il giorno, magari lo usiamo anche al posto dell'orologio e la sera ci piacerebbe continuare ad usarlo come telecomando davanti alla tv. Impossibile? No si può fare e non occorre molto, neanche la porta a infrarossi, grazie a un progetto opensource realizzato da Luca Cassioli **(http://code.google.com/p/ledrem/source/browse)**.

:: Cosa occorre

Ogni telefonino recente dispone infatti di una presa per auricolare che è a tutti gli effetti un canale trasmissivo a due linee (ma è consigliabile usare un telefono con presa audio stereo). Grazie a questo canale e un minimo di impegno è possibile aggiungere gli infrarossi necessari a pilotare, ad esempio, un videoregistratore.

Prima di procedere occorrono:

- un telefono con uscita audio stereo (positivo, negativo, ground) o uscita simmetrica (audio+/audio-)
- due led a infrarossi
- un pc con scheda audio
- una vecchia cuffia audio a jack da sacrificare
- un software di registrazione audio sul pc
- un software di editing audio sul pc

È indifferente la piattaforma software sottostante, quindi sentitevi liberi di usare Windows, Mac o Linux.

:: Acquisiamo i comandi

Per poter trasformare il telefonino in un telecomando universale dobbiamo renderlo in grado di inviare i comandi, ma prima dobbiamo averli! Tagliamo dalla vecchia cuffia audio gli auricolari e recuperiamo il cavo collegato al jack. Al posto degli auricolari montiamo uno dei led. Anche senza avere o saper usare un saldatore è possibile fissare il led il tempo necessario a registrare i comandi, ad esempio con del nastro adesivo o piccoli coccodrilli da laboratorio.



I cavo audio stereo con jack è costituito da tre fili: positivo, negativo e ground.

Inseriamo il cavo nella scheda audio (ingresso microfono) e lanciamo il programma di registrazione sul PC (es. Audacity). Come frequenza impostiamo 76000Hz (a 16 o 32 bit).

Ora prendiamo il telecomando di cui vogliamo copiare il comportamento, lo mettiamo di fronte al led e premiamo il tasto che vogliamo copiare (es. accensione). Il telecomando illuminerà con il suo led il nostro che trasdurrà il segnale e la scheda audio effettuerà il campionamento che ci ritroveremo come file wav. A. Appena lasciamo il bottone sul telecomando, interrompiamo la registrazione sul software.



Per intercettare il comando inviato, gli elementi vanno disposti con estrema precisione nel modo raffigurato.

Dal momento che il segnale è davvero rapido (siamo sui millisecondi) dovremo fare diversi zoom per vedere la sequenza chiaramente, sia in ampiezza che in larghezza. Ciò che vedremo è il comando codificato tramite protocollo SIRC (www.sbprojects.com/knowledge/ir/sirc.htm) e con un po' di pazienza saremo in grado di leggere i bit trasmessi.

:: Editing del comando

Nel blog Jumping Jack Flash è descritto in dettaglio il complesso editing manuale del comando acquisito (jumpjack.wordpress.com/2008/05/22/remote-control-3-editing-waveform) che permette di ricostruire la sequenza originale di bit. Un metodo sicuramente più comodo è quello di generare direttamente il comando come sequenza di bit e creare con SOX (sox.sourceforge.net) il file audio (vedi www.planetmobile.it/jumpjack/LedRem/batches3.zip).

In entrambi i casi non è possibile mandarlo semplicemente in play per replicarlo perché il segnale va trasmesso a 38000Hz mentre la maggior parte delle schede audio trasmette segnali audio solo fino a circa 20000Hz. Fortunatamente è stato rilasciato un brevetto, liberamente utilizzabile, su come usare dei canali audio a 19000Hz per generare un segnale a 38000Hz (www.freepatentsonline.com/6931231.html); brevemente: vanno connessi i due led uno opposto all'altro, uno sul canale positivo e uno sul canale negativo; il segnale andrà trasmesso a 19000Hz ma il circuito così realizzato sommerà i due segnali realizzando un segnale a 38000Hz (la portante).

Sempre grazie a Audacity è possibile realizzare senza difficoltà il segnale stereo così descritto, creando due canali mono che trasmettono lo stesso segnale in opposizione di fase.

:: Trasmissione

Riprendiamo ora il cavo audio, trascurando il conduttore di ground e connettendo i led opposti tra loro solo tra il canale destro e sinistro del cavo. Posizionando il cavo in prossimità del dispositivo (es. videoregistratore) e mandando in play il segnale stereo dovremmo ottenere il risultato atteso (accensione!).

A questo punto va ripetuta la procedura per ogni comando che vogliamo replicare, salvando ciascuno in un file wav (codificato PCM, 32 bit, 48000Hz). Ora dobbiamo connettere i led al telefonino come abbiamo fatto per il pc e magari non c'è un'uscita audio a jack! Non disperiamo, per le prove va bene un classico Nokia dotato di pop-port (tutti i modelli recenti vanno bene, vedi box). Il circuito prevede una resistenza da



Così viene rappresentata graficamente dall'interfaccia del software Audacity la traccia dei bit del comando intercettato.

10 ohm, ma da alcune prove fatte non sembra essere strettamente necessaria. i led andranno connessi tra i pin 12 e 13, il pin 13 in corto con 11 e ground. In questo modo mandando in play il file dal telefonino (chiaramente il telefonino deve avere abbastanza memoria per contenere i file wav e un player in grado di riprodurli) verrà generato il comando come farebbe un telecomando, tramite i led. Se il terminale che usiamo ha symbian si può anche automatizzare l'invio dei comandi arrivando a pilotare il dispositivo da remoto per chiedergli di programmare ad esempio la videoregistrazione di un programma via sms. Abbiamo creato un robot radiocomandato!

Massimiliano Brasile

NOKIA COMPATIBILI

N72, 3250 XpressMusic, 5500 Sport, E50, E61, E61i, E70, N73, N91, N92, N93, N93i, 6110 Navigator, 6290, E90, N76, N95, 7710, 3230, 7610, 6630, 6680, N70, N90.